T.C.
SAKARYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

LALE: YENİ BİR HAFİF SİKLET BLOK ŞİFRELEME ALGORİTMASI TASARIMI

YÜKSEK LİSANS TEZİ

Fatma Betül PAK

Matematik Anabilim Dalı

Cebir ve Sayılar teorisi Bilim Dalı

TEMMUZ 2023

T.C.
SAKARYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

LALE: YENİ BİR HAFİF SİKLET BLOK ŞİFRELEME ALGORİTMASI TASARIMI

YÜKSEK LİSANS TEZİ

Fatma Betül PAK

Matematik Anabilim Dalı

Cebir ve Sayılar teorisi Bilim Dalı

Tez Danışmanı: Prof. Dr. Mehmet ÖZEN

TEMMUZ 2023

Fatma Betül PAK tarafından hazırlanan "LALE: Yeni Bir Hafif Siklet Blok Şifreleme Algoritması Tasarımı" adlı tez çalışması 11.07.2023 tarihinde aşağıdaki jüri tarafından oy birliği ile Sakarya Üniversitesi Fen Bilimleri Enstitüsü Matematik Anabilim Dalı Cebir ve Sayılar teorisi Bilim Dalı'nda Yüksek Lisans tezi olarak kabul edilmiştir.

Tez Jürisi

Jüri Başkanı : **Prof. Dr. Mehmet ÖZEN** (Danışman)
Sakarya Üniversitesi

Jüri Üyesi : **Doç. Dr. Ünal ÇAVUŞOĞLU**
Sakarya Üniversitesi

Jüri Üyesi : **Doç. Dr. Hakan ADIGÜZEL**
Sakarya Uygulamalı Bilimler Üniversitesi

ETİK İLKE VE KURALLARA UYGUNLUK BEYANNAMESİ

Sakarya Üniversitesi Fen Bilimleri Enstitüsü Lisansüstü Eğitim-Öğretim Yönetmeliğine ve Yükseköğretim Kurumları Bilimsel Araştırma ve Yayın Etiği Yönergesine uygun olarak hazırlamış olduğum "LALE: Yeni Bir Hafif Siklet Blok Şifreleme Algoritması Tasarımı" başlıklı tezin bana ait, özgün bir çalışma olduğunu; çalışmamın tüm aşamalarında yukarıda belirtilen yönetmelik ve yönergeye uygun davrandığımı, tezin içerdiği yenilik ve sonuçları başka bir yerden almadığımı, tezde kullandığım eserleri usulüne göre kaynak olarak gösterdiğimi, bu tezi başka bir bilim kuruluna akademik amaç ve unvan almak amacıyla vermediğimi ve 20.04.2016 tarihli Resmi Gazete'de yayımlanan Lisansüstü Eğitim ve Öğretim Yönetmeliğinin 9/2 ve 22/2 maddeleri gereğince Sakarya Üniversitesi'nin abonesi olduğu intihal yazılım programı kullanılarak Enstitü tarafından belirlenmiş ölçütlere uygun rapor alındığını çalışmamla ilgili yaptığım bu beyana aykırı bir durumun ortaya çıkması halinde doğabilecek her türlü hukuki sorumluluğu kabul ettiğimi beyan ederim.

18/07/2023

Fatma Betül PAK

Sevgili aileme…

TEŞEKKÜR

Yüksek Lisans eğitimim boyunca beni teşvik eden, titizlikle yönlendiren ve değerli bilgi ve deneyimlerini benimle paylaşan kıymetli danışman hocam Prof. Dr. Mehmet ÖZEN'e teşekkürlerimi sunarım. Tez çalışmalarımda yol gösteren, bilgi ve deneyimlerini benimle paylaşan ve yardımlarını benden esirgemeyen değerli hocam Doç. Dr. Ünal ÇAVUŞOĞLU'na teşekkürlerimi bir borç bilirim.

Ayrıca hayatım boyunca maddi ve manevi desteklerini benden esirgemeyen, her zaman yanımda olan kıymetli babama ve anneme, her türlü desteği için sevgili ablama ve kardeşime çok teşekkür ederim.

Son olarak Yüksek Lisans eğitimim süresince aldığım BİDEB 2210-A bursu için TÜBİTAK'a teşekkürlerimi sunarım.

Fatma Betül PAK

İÇİNDEKİLER

Sayfa

KISALTMALAR

3DES : Triple Data Encryption Standard
AES : Advanced Encryption Standard
ARX : Add-Rotate-XOR
DES : Data Encryption Standard
FN : Feistel Network
GE : Gate Equivalent
GFN : Generalized Feistel Network
IOT : Internet of Things
LAN : Local Area Network
MDS : Maximum Distance Separable
NIST : National Institute of Standards and Technology
NLFSR : Nonlinear-Feedback Shift Register
RAM : Random Access Memory
RFID : Radio-Frequency Identification
ROM : Read-only Memory
RSA : Ronald, Shamir, Adleman
S-BOX : Substitution Box
SPN : Substitution-Permutation Network
TLS : Transport Layer Security
WLAN : Wireless Lan
WPA : Wi-Fi Protected Access
XOR : Exclusive-OR Operation
DNA : Deoksiribo Nükleik Asit

SİMGELER

e_k	: Şifreleme fonksiyonu
d_k	: Deşifreleme fonksiyonu
x	: Açık metin
y	: Şifreli metin
k	: Anahtar
K	: Anahtar uzayı
s_i	: Anahtar dizisi
ΔX	: Girdi farkı
ΔY	: Çıktı farkı
p_L	: Lineer yaklaşım olasılığı
$\mathbf{Pr}$	: Olasılık
P_l	: 64-bit açık metin
WK	: 64- bit beyazlatma anahtarı
S	: 4x4 S-box
P	: 64-bit permütasyon
$A \| B$	: A ve B bit dizilerinin ard arda bağlanması
F	: Çevrim fonksiyonu
RC_i	: i. çevrimde kullanılan 32-bit Çevrim sabiti
RK_i	: i. çevrimde kullanılan 32-bit Çevrim anahtarı
$>> \mathbf{13}$	: 13-bit Sağ çevrimsel kaydırma işlemi
$\mathbf{Pr}$	: Olasılık
C	: 64-bit şifreli metin
$\oplus$	: Bit bazında özel-OR işlemi (XOR)

TABLO LİSTESİ

Sayfa

ŞEKİL LİSTESİ

Sayfa

LALE: YENİ BİR HAFİF SİKLET BLOK ŞİFRELEME ALGORİTMASI TASARIMI

ÖZET

Teknolojide son dönemde yaşanan büyük gelişmeler ile veri güvenliğini sağlamak önemli bir sorun haline gelmiştir. Tarihi çok eskiye dayanan Kriptoloji bilimi, insanların güvenli bir şekilde haberleşmesi, veri aktarması ya da verileri depolaması için ortaya çıkmış bir bilim dalıdır. Geliştirilen şifre sistemlerin en temel amacı gizliliği önem arz eden verileri saklamak ya da iletmektir. Bugüne kadar veri güvenliğini sağlamak için birçok tarihi ve modern şifre sistemleri tasarlanmıştır. Geleneksel şifreleme algoritması olarak bilinen bu şifreleme sistemleri kaynak yönünden zengin cihazlarda, büyük verilerin şifrelenmesinde kullanılır. Ancak bu algoritmalar IOT gibi kaynak yönünden kısıtlı cihazlar için enerji tüketimi anlamında kullanıma uygun değildir. Bu durumda Hafif kriptografi etkili bir çözümdür.

Hafif kriptografi algoritmaları, kaynak kısıtlı cihazlarda ihtiyaç duyulan performans ve güvenliği sağlayan şifreleme sistemleridir. Bugüne kadar geliştirilmiş Hafif kriptografi sistemleri incelendiğinde, sistemlerde farklı tasarım yöntemleri tercih edildiği, bu sebeple birbirinden farklı performans ve güvenlik özelliklerine sahip sistemler elde edildiği gözlemlenmiştir. Genel olarak bir şifreleme sisteminin tasarımında, bu sistemlerin en önemli kullanım sebebi olan güvenlik ön planda tutulmaya çalışılır. Ancak Hafif kriptografi şifreleme sistemlerinin daha çok küçük cihazlar için geliştirilmesi ve bu cihazların kaynak yönünden kısıtlı olmaları nedeniyle böyle cihazlarda güvenliği sağlamanın yanında hızlı olması ve enerji tüketiminin en az seviyede olmasını sağlamak gerekmektedir. Bugüne kadar geliştirilen Hafif şifre sistemleri de bu amaçla tasarlanmıştır. Ancak yapılan performans ve güvenlik ölçümleri karşılaştırması sonuçlarına göre sistemlerin yeterli güvenlik seviyesini sağlarken performans açısından iyi olmadığı ya da performans açısından iyi durumda iken güvenlik yönünden zayıf olduğu ortaya çıkmaktadır.

Bu tez çalışmasının amacı, Nesnelerin İnterneti (IOT) gibi kaynak kısıtlı cihazlarda güvenliği sağlayan, performans açısından iyi olan yeni bir Hafif şifre sistemi tasarlamak ve ölçümlerini yapmaktır. Bilinen en güçlü analitik saldırı çeşitlerinden biri olan diferansiyel kriptanaliz, İntegral saldırısı ve Kendine benzerlik saldırısı yapılarak LALE'nin güvenlik ölçümleri yapılmıştır. Yeni şifre sistemi, bu saldırılara karşı oldukça güvenlidir. Sistemin güvenliğinde önemli rolü olan S-box katmanının tasarımı için DNA şifreleme tabanlı yepyeni bir yöntem geliştirilmiştir ve bu yöntem ile yeni bir 4x4 S-box tasarlanmıştır. Yeni Hafif şifre sistemi tasarımımızın yazılım uygulaması yapılarak şifreleme ve deşifreleme süreleri ve RAM ölçümleri yapılmışıtır. Buna göre LALE, AES gibi bilindik diğer şifre sistemlerine göre daha hızlıdır.

LALE: A NEW LIGHTWEIGHT BLOCK ENCRYPTION ALGORİTHM DESIGN

SUMMARY

The Internet of Things (IoT) is one of the most important technology which will interact the human world with the every machine. IOT is used in transport, logistics, environment, infrastracture which are smart (such as smart cities, smart malls, smart homes and industry 4.0), smart healthcare and agriculture, RFID tags, sensor nodes, battery operated portable devices and medical implants and many more. The definition of IOT can be expressed as a network of connected devices, which have their own unique identification. It can collect and interchange data through the network whether any human interference or not.

When billions of connected devices are working together, particularly when transferring the data from server to sensors, it leads to many kinds of problems to users such as interoperability, privacy, longevity, and much more. As IOT devices are easily available and interact with the material world to accumulate private data, that makes them an tempting target to attackers and exposed to various security attacks. Hence cybersecurity gain prominence in IOT.

With the recent big developments in technology, ensuring data security has become an important issue. Cryptology, which dates back a long time, is a branch of science that has emerged for people to communicate, transfer data or store data securely. Cryptography is a great solution to enhance the security of the stored data over the internet. However, conventional cryptography algorithms which are appropriate for PCs and have high resource requirement can't be adopted for IOT devices which are resource-constrained. With the introduction of AES, it become an remarkable and preferred option for some applications of block ciphers. As resource-constrained IOT devices have power, size and memory constraints, AES is often inproper for them. In these circumstances Lightweight Cryptography is an effective solution. Lightweight Cryptography algorithms are encryption systems that provide the performance and security trade-off which is needed in resource-constrained devices. Hence, in the last years many researches have been conducted based on lightweight ciphers by researchers. Especially on designing lightweight blockciphers with particularly low implementation costs and analyzing them has drawn significant attention.

Lightweight cryptography algorithms have the following three foundamental properties. When cryptography is applied to any IOT device which is resource constrained, performance, cost and security are the main properties. By using simple round functions on the small block using a small key with simple key scheduling, LWC algorithms satisfy the performance and cost properties. With the adoption of one of the six internal structures (SPN, FN, Hybrid, GFN, NLFSR, ARX) LWC algorithms

satisfy the last and important property which is security, to resist against the security attacks. While constructing the round function, the size of its components, S-box, how and at what stage the round constant addition will be, the type of permutation, or the type of the key sheme, size of the key and the block, and of course the internal structure part, etc. different choices in algorithms induce different properties. These properties leads to various consequences in algorithms.

When compared the lightweight algorithms in terms of performance, some results were obtained. Speck and Simon algorithms are the best when compared with other lightweight algorithms in terms of software efficiency. At memory requirements, Simon and Speck are again leading with 200 bytes of ROM and 0 bytes of RAM. In terms of Hardware efficiency, Midori and Piccolo are the leading ones. SEA and Hummingbird algorithms are the best when compared the effect of block and key length in hardware. When compared in terms of Physical area requirement, Ktantan requires only 462 GE, and Print cipher comes in second place with 503 GE. Moreover in terms of energy comsumption, Midori, Piccolo and Prince are respectively the best, with small differences. When we look at the comparisons in terms of performance, it is obvious that there is no algorithm that is good in every field. For example Simon has good results in software efficiency and memory requirements but it is not good in terms of energy cunsumption. When compared in terms of security, all algorithms are vulnerable to various attacks. Hence the choices made during the design phase cause different results.

The aim of this these is presenting a new lightweight block cipher which is easily adoptable in resource constrained devices. Before making our new design, many lightweight algorithms in the literature were examined. There are many lightweight cryptography algorithms on the market. However most algorithms are unable to achieve the balance between the energy consumption and security. When these algorithms were examined, we observed that the differences of the components used in their content, make algorithms advantageous in certain aspects, while disadvantaging them in many other fields. Considering these reviews, a brand new algorithm has been obtained that balances safety, energy and cost, each component of which has been designed carefully.

Components of the new proposed cipher, such as Substitution layer, Key Scheduling, Permutation layer, etc. was designed with security and energy balance in mind. The new cipher's 4x4 S-box is designed in a brand new way which is based on DNA encryption. We have used a key whitening process to increase its resistance against cryptanalytic attacks. Round constant addition part has also been carefully chosen to maintain the balance of energy and cost. The structure of the new introduced cipher is hybrid structured which is obtained by combining SPN and Feistel Network. An algorithm with optimum value was obtained by using the unique features of SPN and Feistel structure together.

Our new introduced cipher provides 64-bit block in order to make it suitable for standard applications and 128-bit key to achieve the required security level. The structure of the cipher is in Hybrid type which combines the SPN and the Feistel Network. The structure of other lightweight algorithms is generally preferred as SPN or Feistel Network. However, these two structures have their own advantages and

disadvantages. Substitution Permutation Network and Feistel Network are the famous structures of block ciphers thanks to their adaptability to application necessity. Round function is applied to only one half of the block in Feistel structures and they can be implemented with low power in hardware. As Feistel type structures introduce such a nonlinearly round function, such constructions usually require more enforcement of round functions to sustain the security level as compared to SPN structures. For this reason, the structure of the cipher was preferred as a hybrid structure where we can use the features of SPN and Feistel Network.

In the light of those informations we have used a new approach at designing the new cipher. SPN and Feistel Network is combined with low number of rounds which enables us to achieve high security level. The decryption and encryption function of the new introduced cipher is quite similar. Hence LALE has roughly the same physical requirements to implement encryption and decryption.

LALE's round number is 10-2 which achieves the high security level. 10-2 round means that the round number of SPN part is 10, and number of rounds of the Feistel part is 2. Accordingly, it is necessary to apply the 10-2 round version of the cipher for security purposes to devices that are resource-limited, such as IoT. If desired, in other large devices or systems, a structure with the round of 12-2 or 16-2 should be applied for advanced safety purposes. Likewise if desired, in other IOT devices for low energy usage and speed, a structure with round of 8-2 should be applied.

Various attacks have been applied to measure the security of the new encryption system, which is 10-2 round. According to the result of the differential attack, the new 10-round encryption system provides a sufficient level of security. It seems that the factors that increase the system's resistance to integral attack and self-similarity attacks are found in the new healing system, so it is safe against these attacks. We make the performance measurement of the new cipher by making its software implementation with C++. We measure the encryption and decryption times of our new introduced cipher LALE. The results of our new introduced cryptography algorithm LALE is given in a table. At the same time, we have compared LALE with other cryptographic systems in terms of encryption and decryption times. According to the results obtained, the new introduced system is faster than some other algorithms like AES, Lblock, Present and Piccolo. We also did the RAM measurement and give it in a table.

1. GİRİŞ

Bilgi, insanlık için her zaman önemli olmuştur. Günümüzde kullanılan son model cihazlar ve ağ teknolojisi sayesinde bilgiye ulaşmak son derece kolaylaşmıştır. Ancak bilginin kolay ulaşılabilir olması, saklanırken ya da bir yerden bir yere gönderilirken açığa çıkan güvenlik zaafiyeti önemli bir sorun olarak karşımıza çıkmaktadır [1]. Kriptoloji bu ihtiyaca binaen ortaya çıkmış bir bilim dalıdır. Kriptoloji'nin bir dalı olan kriptografi, önem arz eden verileri ya da dosyaları şahıslar arasında transfer ederken ya da herhangi bir yerde depolarken bu işlemlerin güvenli olarak yapılması işlemini birtakım algoritmalar tasarlayıp uygulayarak sağlayan bir bilimdir.

Özellikle son yıllarda adını sıkça duyduğumuz, çeşitli alanlarda kullanılan Nesnelerin İnterneti (IOT) cihazları toplumun her kesiminde yaygın bir şekilde kullanılmaktadır. Nesnelerin İnterneti, insan yaşamını makinelerle bütünleştiren son teknolojidir [2]. Nesnelerin İnterneti, akıllı ulaşım & tedarik, sağlık, çevre, yapı (akıllı şehirler, evler, ofisler, alışveriş merkezleri, endüstri 4.0, vb.), akıllı tarım [3], RFID etiketleri, sensör düğümleri, tıbbi cihazlar, bataryalı taşınabilir cihazlar [4] ve birçok alanda çeşitli uygulamalarla yaygın olarak kullanıldığı için oldukça popülerdir. IOT, kendine has özellikleriyle insan etkileşimli olan ya da olmayan internet aracılığıyla bilgi toplayıp değiştirebilen bağlantılı cihazlardan oluşan bir ağdır [3].

Milyonlarca cihazın bağlantılı bir şekilde çalıştığı bir ortamda kullanıcılar güvenlik & gizlilik, cihazların birlikte çalışabilmesi, uzun ömürlülük ve destek gibi birçok konuda zorluk yaşayabilirler [3]. IOT cihazları özel bilgi toplamak ve çevrede olup biteni kontrol etmek için dış dünya ile doğrudan etkileşim kurduklarından kolay ulaşılabilir ve saldırıya açık haldedirler ki bu, saldırganlar için oldukça cazip bir durumdur [3]. Dolayısıyla IOT için siber güvenlik büyük bir öneme sahiptir. O halde kriptografi, belleğe alınmış ya da ağ üzerinden takas edilen bilgiyi güvende tutmak için iyi bir çözümdür. Ancak geleneksel kriptografinin uygulanması için gereken kaynak ihtiyacının fazla olması, kaynak kısıtlı IOT cihazları için uygun olmadıkları anlamına gelmektedir.

AES' in icadıyla birlikte yeni bir blok şifre ihtiyacı ortadan kalkmıştır çünkü hemen hemen her blok şifre uygulaması için AES mükemmel bir seçimdir [5]. Ancak kaynak kısıtlı IOT cihazlarının boyut, güç ve hafıza gibi kısıtları olduğu için AES gibi sistemler bu cihazlara uygun değildir [6]. Dolayısıyla son yıllarda Hafif Kriptografi üzerine yapılan çalışmalar büyük önem kazanmıştır. Geleneksel kriptografi ile kıyaslandığında Hafif Kriptografi' nin üç temel özelliği vardır. Herhangi bir IOT cihazına kriptografiyi uyarlarken fiziksel maliyet, performans ve güvenlik özelliklerini taşıyıp taşımadığına dikkat etmeliyiz. İlk iki özellik Hafif algoritmada küçük blok boyu ve basit anahtar şeması ile üretilmiş küçük anahtar kullanan basit çevrim fonksiyonu bulundurmak suretiyle sağlanır. Sonuncu özellik olan güvenlik için altı iç yapı çeşidinden herhangi birinin (SPN, FN, GFN, ARX, NLFSR, Hibrit) sisteme uyarlanması gerekmektedir. Dolayısıyla uygulama maliyeti düşük Hafif algoritmalar tasarlamak [7] ve analizini yapmak [8] son yıllarda büyük önem kazanmıştır [7].

1.1. Literatür Taraması ve Tezin Amacı

Bugüne kadar birçok Hafif Kriptografi algoritması tasarlanmıştır. Bu Hafif Kriptografi algoritmalarından bazıları ASCON V1 [9], CLEFİA [10], FeW [11], GRANULE [12], Hummingbird [13], ITUbee [14], IDEA [15], KATAN/KHANTAN [16], Klein [17], LBlock [18], LİCİ [2], Midori [4], Noekeon [19], Present [5], Prince [7], Print [20], Piccolo [8], Rectangle [21], Simon [22], SPECK [23], TEA [24] ve Twine [6] şeklindedir. Algoritmaların performans ve güvenlik açısından karşılaştırmaları incelendi. Buna göre yazılım uygulaması, hafıza gereksinimi, donanım etkisi, blok ve anahtar uzunluğunun donanıma etkisi, alan ve enerji gereksinimi gibi alanlarda yapılan karşılaştırmalar incelendiğinde her algoritmanın farklı alanda iyi olduğu gözlemlendi. Dolayısıyla bu sonuçlara göre, her alanda iyi durumda olan bir algoritma ile karşılaşılmadı. Güvenlik açısından değerlendirmelere bakıldığında ise her algoritmanın farklı bir saldırı çeşidine karşı dayanıksız olduğu gözlemlendi.

Bu tez çalışmasında, mevcut Hafif Kriptografi algoritmalarından daha güvenli ve performanslı çalışan, IOT cihazlarında kullanımı uygun olan bir şifre sistemi tasarlamak amaçlanmıştır. Yeni şifre sistemini tasarlarken algoritmanın cihaza

uygulandığında maliyet anlamında düşük, hız anlamında yüksek ve güvenlik olarak iyi düzeyde olan bir şifre sistemi tasarlamak hedeflenmiştir.

1.2. Tezin İçeriği

Bu tez çalışması beş bölümden oluşmaktadır. Giriş bölümünden sonra verilen ikinci bölümde bazı cebirsel tanımlar ve kriptoloji ile ilgili temel kavramlar verilmiştir. Bölümün devamında kriptografi ve kriptanaliz' in içeriğinden bahsedilmiştir.

Üçüncü bölümde Nesnelerin İnterneti ve Hafif Kriptografiden bahsedilmiştir. Devamında ise yeni bir Hafif Kriptografi sistemi tasarlarken göz önünde bulundurulması gereken bazı ölçütler verilmiştir.

Dördüncü bölümde ise tasarlanılan yeni Hafif şifre sistemi LALE'nin içeriği ve tasarım ölçütleri verilmiştir. Ardından, yeni algoritmanın güvenlik analizleri verilmiştir. Devamında ise sistemin performans analizi ve sonuçlarından bahsedilmiştir.

Beşinci bölümde Sonuçlar ve Öneriler verilerek tez çalışması tamamlanmıştır.

2. TEMEL KAVRAMLAR

2.1. Cebirsel Tanımlar

İlk kısımda tezde kullanılacak olan bazı cebirsel tanım ve teoremler verilecektir. Aşağıdaki tanım ve teoremler [25-29] numaralı kaynaklardan referans alınarak hazırlanmıştır.

Tanım 2.1.1. S boştan farklı bir küme olsun. $*: S \times S \to S$ fonksiyonu S'de bir ikili işlemdir. Özel olarak, $*$ S'de bir ikili işlem olsun. $x, y \in S$ için $x * y$ ifadesi (x, y) nin $*$ altındaki görüntüsüdür.

Tanım 2.1.2. k sıfırdan farklı bir tamsayı ve $x, y \in \mathbb{Z}$ olmak üzere,

$$x \equiv y (\text{mod } \text{k}) \Rightarrow \text{k} \mid x - y$$

ise özel olarak bu ifadeye, x, y tamsayıları mod k ya göre denktirler denir.

Tanım 2.1.3. (Bölme Algoritması) $x, y \in \mathbb{Z}$ ve $x \neq 0$ olsun. O halde, $0 \leq s < |x|$ iken $y = xt + s$ eşitliğinde bölme algoritmasına göre tek türlü belirli t ve s tamsayıları vardır.

Tanım 2.1.4. x ve y sıfırdan farklı birer tam sayı olmak üzere,

i) Herhangi bir $b > 0$ tamsayısı için $b \mid x$ ve $b \mid y$ oluyorsa b ye x ile y nin bir ortak böleni denir.

ii) b, x ile y nin bir ortak böleni olsun. O halde x ile y nin bir ortak böleni p olmak üzere, en büyük ortak bölenleri (e.b.o.b) $p \mid b$ olacak şekilde b tamsayısıdır. Ayrıca bu ifade $(x, y) = b$ ile gösterilir.

Teorem 2.1.1. s,t sıfırdan farklı herhangi iki tam sayı olmak üzere bu iki tamsayının her zaman bir en büyük ortak böleni vardır ve $b=(s,t)$ iken $b=us+vt$ olacak şekilde $\exists u,v\in\mathbb{Z}$ bulunur.

Tanım 2.1.5. $\mathbb{Z}$ de denklik bağıntısı ile belirtilen, k modülüne göre $(\mathrm{mod}\,k)$ kalan sınıfları kümesinin tamamı $\mathbb{Z}_k$ ile gösterilir.

Önerme 2.1.1. k asal bir tamsayı olsun. Bu durumda, sıfırdan farklı olmak üzere, her elemanın tersi $\mathbb{Z}_k$ da vardır.

Tanım 2.1.6. $*$, boştan farklı bir K kümesinde ikili işlem olmak üzere, $(K,*)$ cebirsel yapısının aşağıdaki şartları sağlaması durumunda bu yapıya bir grup denir.

$K1$: $*$, K de bir ikili işlemi ifade eder.

$K2$: K da $*$ işlemi birleşme özelliğini sağlasın. O halde $\forall x,y,z\in K$ için, $x*(y*z)=(x*y)*z$ dir.

$K3$: K da $*$ işleminin birim elemanı vardır. O halde $\forall k\in K$ için $k*b=b*k=b$ eşitliğini sağlayacak şekilde $\exists b\in G$ vardır.

$K4$: K da $*$ işlemine göre, her elemanın bir tersi mevcuttur. Yani $k\in K$ için, $k*k^{-1}=k^{-1}*k=b$ eşitliğini sağlayacak şekilde $\exists k^{-1}\in G$ vardır.

Tanım 2.1.7. $(K,*)$ bir grup olmak üzere eğer $\forall m,n\in K$ için $m*n=n*m$ ise bu yapıya değişmeli bir grup veya Abel grubu denir.

Tanım 2.1.8. K boştan farklı bir küme ve bu küme üzerinde tanımlı iki ikili işlem $+$ ve $\cdot$ olsun. Eğer $(K,+,\cdot)$ yapısı belirtilen şartları sağlıyorsa K bir halkadır.

K_1 : $(K,+)$ bir abelyen grup.

K_2 : Çarpma birleşmelidir.

K_3 : Her $x, y, z \in K$ için $x \cdot (y+z) = (x \cdot y) + (x \cdot z)$ soldan dağılma özelliği ve $(x+y) \cdot z = (x \cdot z) + (y \cdot z)$ sağdan dağılma özelliği sağlanır.

Tanım 2.1.9. $(K, +, \cdot)$ yapısı bir halka olsun. Halkanın birim elemanı, ikinci işleme göre etkisiz eleman olması durumunda mevcuttur ve 1_K ile gösterilir. Özel olarak bu halka birimli halka olarak adlandırılır. Eğer ikinci işleme göre halkada değişme özelliği sağlanıyorsa halka değişmeli halka olarak adlandırılır.

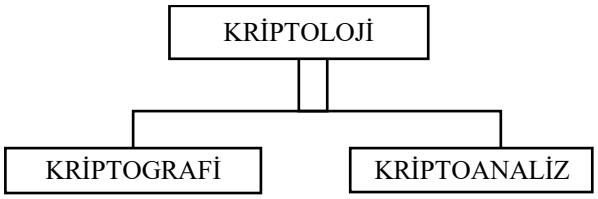
Tanım 2.1.10. K birimli ve değişmeli bir halka olmak üzere, $K - \{0_K\} = K^*$ sıfırdan farklı elemanların bulunduğu kümede her elemanın tersi varsa K ya bir cisim denir.

Önerme 2.1.2. p asal ise $\mathbb{Z}_p$, p elemanlı bir cisimdir.

Tanım 2.1.11. C bir cisim olmak üzere eğer C cisminin eleman sayısı sonlu ise, C cismine sonlu cisim ya da Galois cismi denir.

2.2. Kriptoloji

Kriptoloji, temelleri çok eskiye dayanan bir bilim dalıdır. Bu bilimin ilk temelleri M.Ö. 2000 yılında Antik Mısır'da atılmıştır [30]. Yani insanlık için bilginin gizliliği çok eski bir ihtiyaçtır ve çözümü de yine çok eskidir. Kriptoloji kelimesi terim olarak ilk kez 1844 yılında kullanılmıştır [31]. Bu kelime köken olarak Yunanca'da yer alır ve dilimize 'Şifre Yazımı' olarak tercüme edilir [30]. Kriptoloji gizliliği önem arz eden bilgilerin bir yerden başka bir yere gönderilirken, bir yerde saklanırken veya



Şekil 2.1. Kriptoloji'nin genel görünümü.

depolanırken çeşitli algoritmaların kullanılarak şifrelenmesi işlemini kapsayan bir bilim dalıdır. Kriptoloji bilimi Kriptografi ve Kriptanaliz olmak üzere ikiye ayrılır.

2.2.1. Kriptografi

Kriptografi, mesajın anlamını gizlemek amacıyla mesajı gizli bir şekilde yazma bilimidir [32]. Bu bilimin amacı güvenliği yüksek şifreleme sistemleri tasarlamaktır. Bu sistemler çeşitli matematiksel işlemlerin ya da fonksiyonların bir arada kullanılmasıyla elde edilirler.

Bir Kriptosistem aşağıdaki şartları sağlayan (M, S, A, E, D) beşli parametresine bağlıdır:

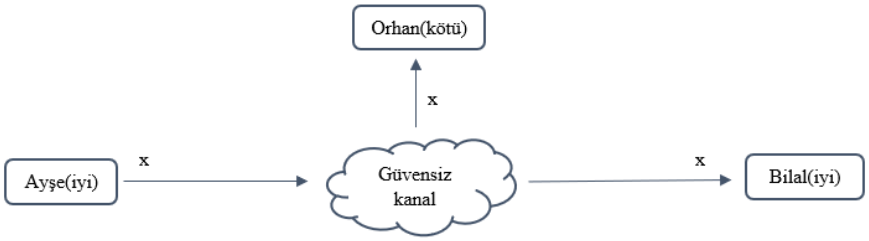
1. M mümkün olan tüm açık metinlerin sonlu kümesidir.
2. S mümkün olan tüm şifreli metinleri bulunduran sonlu kümedir.
3. A mümkün olan tüm anahtarlardan oluşan anahtar uzayıdır.
4. Her $k \in A$ için $e_k \in E$ şifreleme yöntemi ve buna karşılık bir $d_k \in D$ deşifreleme yöntemi vardır. Her $x \in M$ açık metni için $e_k : M \to S$ ve $d_k : S \to M$ fonksiyonları $d_k(e_k(x)) = x$ şartını sağlar [33].

Şekil 2.2. Kriptografi' nin yapısı.

Kriptografi, Simetrik şifreleme, Asimetrik şifreleme ve Protokoller olmak üzere üçe ayrılır. Bu bölümde bu başlıkların içeriğinden ayrıntılı bir şekilde bahsedilmiştir. Aşağıdaki bölüm [32-36] numaralı kaynaklardan referans alınarak hazırlanmıştır.

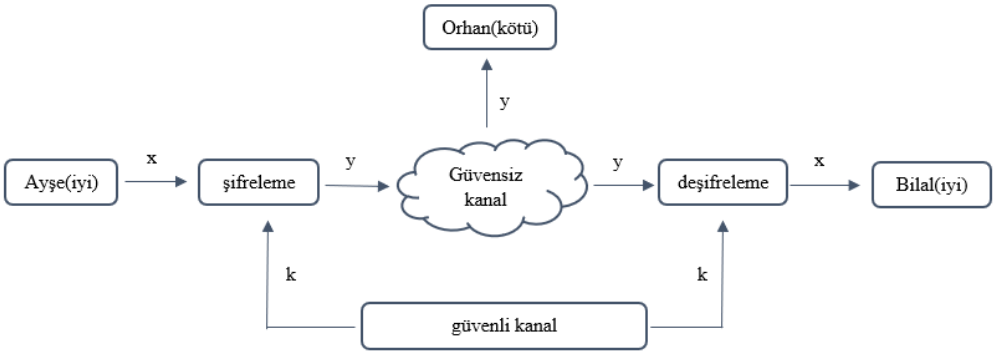
2.2.1.1. Simetrik şifreleme

Simetrik Şifreleme tekniğinde iki tarafın bir şifreleme ve deşifreleme yöntemi ve ortak bir gizli anahtarı vardır. Simetrik Kriptografik Sistemler bazen simetrik anahtarlı, gizli anahtarlı ya da tek anahtarlı algoritma olarak da adlandırılır. Simetrik Kriptografiyi basit bir problem üzerinden açıklarsak: Ayşe ve Bilal isminde iki tane kullanıcı güvensiz kanal üzerinden haberleşmek istesinler. Kanal kelimesi ile internet, cep telefonu ya da LAN (Local Area Network) iletişim araçları kastedilmiştir. Şekil 2.3'te gösterildiği gibi Orhan ise, Ayşe ve Bilal'i dinlemek üzere kanala erişimi olan kötü niyetli bir kişi olsun. Ancak Ayşe ile Bilal mesajların üçüncü bir şahıs tarafından görüntülenmesini istemesinler.



Şekil 2.3. Güvensiz kanal üzerinden iletişim.

Bu durumda Simetrik Kriptografi güçlü bir çözüm sunar: Şekil 2.4'deki gibi Ayşe, göndermek istediği x açık metnini simetrik bir algoritma kullanarak şifreler ve y şifreli metnini elde eder. Bilal ise y şifreli metnini aldıktan sonra mesajı deşifre ederek x açık metnini elde eder. Bu aşamaları yaparken güçlü bir şifreleme algoritması kullanıldığında şifrelenmiş metni elde eden Orhan rastgele bitlerin anlamsızca sıralandığı bir metin ele geçirmiş olur ve amacına ulaşamaz. Böylece Ayşe ile Bilal güvenli bir şekilde iletişim kurabilir.



Şekil 2.4. Simetrik şifreleme ile iletişim.

Kriptografi'de x, y ve k değerleri önemlidir ve

1) x değeri açık metin
2) y değeri şifreli metin
3) k değeri anahtar

olarak adlandırılır. Şifreleme fonksiyonu, açık metni şifreli metne dönüştüren bir dizi işlemlerden oluşur. Deşifreleme işlemi, şifreleme işleminin tersidir ve şifreli metinden açık metin elde etmek için vardır. Sistemde Ayşe ile Bilal arasında anahtar dağıtımı yapan bir güvenli kanal bulunur. Örneğin bu kanal, WLAN'de (Wireless Lan) anahtar dağıtımı yapan WPA (Wi-Fi Protected Access) şifrelemesi olabilir. İlerleyen bölümlerde güvenli anahtar dağıtımı için alternatif bir yöntem verilecektir. Şimdi bir tarihi simetrik şifreleme sistemi olan Öteleme Şifresi' nden bahsedelim.

Öteleme şifresi (Sezar şifresi)

Öteleme Şifresi çok basit bir mantıkla çalışır. Alfabedeki her harf kendisinden belirlenen bir sayı miktarı ötesindeki harf ile yer değiştirir. Örneğin İngiliz alfabesini göz önüne alalım. A harfini 3 pozisyon ötesindeki harf ile değiştirelim, o halde A yerine d gelir. Aynı şekilde B yerine 3 pozisyon ilerisindeki e gelir. Öteleme Şifresi'ni daha iyi anlamak için İngiliz alfabesindeki 26 harfi tablodaki gibi numaralandıralım.

Tablo 2.1. Öteleme şifresi için harfleri numaralandırma tablosu.

Harf	Numara	Harf	Numara
A	0	N	13
B	1	O	14
C	2	P	15
D	3	Q	16
E	4	R	17
F	5	S	18
G	6	T	19
H	7	U	20
I	8	V	21
J	9	W	22
K	10	X	23
L	11	Y	24
M	12	Z	25

Tabloda harfler 0 ile 25 arasında numaralandırılmıştır. Bu Kriptosistem $\mathbb{Z}_{26}$ üzerinde çalışır çünkü İngiliz alfabesinde 26 harf vardır.

Tanım 2.2.1. $x, y, k \in \mathbb{Z}_{26}$ olsun. Bu durumda,

Şifreleme : $e_k(x) = y \equiv x + k \mod 26$

Deşifreleme: $d_k(y) = x \equiv y - k \mod 26$

Örnek: $k = 17$ olsun ve ATTACK kelimesini şifreleyelim.

$a = \text{ATTACK} = a_1, a_2, a_3, a_4, a_5, a_6 = 0,19,19,0,2,10$

$e_{17}(a) = e_{17}(a_1, a_2, a_3, a_4, a_5, a_6) = e_{17}(0,19,19,0,2,10) = (17,10,10,17,19,1)$ = rkkrtb

Bu Kriptosistem için tam anlamıyla güvenlidir diyemeyiz. İki çeşit saldırı yöntemiyle güvenliğini incelersek:

1) Kaba Kuvvet Saldırısı: Bu saldırı çeşidinde seçilen bir (x, y) açık metin-şifreli metin çifti için K anahtar uzayında bulunan olası tüm $k \in K$ anahtarları tek tek denenir ve $d_k(y) = x$ eşitliğini sağlayan k değeri doğru anahtar olarak

kabul edilir. Öteleme Şifresinde $k \in \mathbb{Z}_{26}$ olduğu için olası tüm anahtarların sayısı 26'dır. Anahtar uzayı çok küçük olduğu için günümüz şartlarındaki bir bilgisayarla doğru anahtarı bir saniyeden daha kısa süre içinde bulmak mümkündür.

2) Harf Frekans Analizi: Frekans Analizi, dilin zaman içinde gelişen özelliklerini kullanarak yapılır. İngilizce için konuşursak etkili bir saldırı için aşağıdaki özellikler kullanılır [26,32]:
   1. Elimizdeki şifreli metin kısa olsa bile dilin özelliği korunacaktır ve karakterlerin frekans dağılımı o dilin frekans dağılımına çok yakın olacaktır. Bu yöntemde şifreli metinde en çok tekrar eden harfler belirlenir. Daha sonra en çok tekrar eden harfin yerine frekansı en yüksek olan harf yazılır. Bu şekilde şifreli metinden mantıklı bir metin elde edilmeye çalışılır. Örneğin İngilizce'de en çok tekrar eden harfler sırasıyla %13 ile E, %9 ile T, %8 ile A, … şeklindedir. Tablo 2.2'de İngilizce harflerin Frekans Tablosu verilmiştir.

Tablo 2.2. İngiliz dili harf frekans dağılımı.

Harf	Frekans	Harf	Frekans
A	0,0817	N	0,0675
B	0.0150	O	0,0751
C	0,0278	P	0,0193
D	0,0425	Q	0,0010
E	0,1270	R	0,0599
F	0,0223	S	0,0633
G	0,0202	T	0,0906
H	0,0609	U	0,0276
I	0,0697	V	0,0098
J	0,0015	W	0,0236
K	0,0077	X	0,0015
L	0,0403	Y	0,0197
M	0,0241	Z	0,0007

2. Yukarıda verilen yöntemi genelleştirirsek, dilde en çok tekrar eden ardışık ikili harfler, üçlü harfler, dörtlü harfler, … en çok tekrar eden ardışık ikili, üçlü, dörtlü karakterlerde denenir. Örneğin İngilizce'de Q ile U harfi sıklıkla ardışık şekilde kullanılır.
3. Kelimeleri ayıran boşluklar ile sık tekrar eden kısa kelimeler tespit edilir. Örneğin İngilizce'de THE, AND gibi kelimeler sıklıkla tekrar eder.

Bu üç özellik kullanılarak sistem kırılmaya çalışılır. Öteleme Şifresi'nde Kaba Kuvvet saldırısı ile sistemi kırmak son derece basit olduğu için genelde Harf Frekans Analizi'ne ihtiyaç duyulmaz.

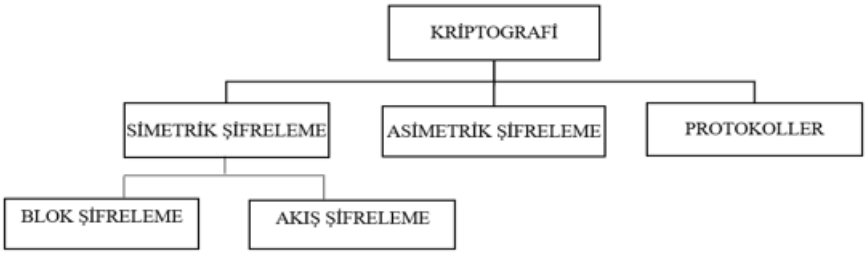
Simetrik bir algoritmada anahtar uzunluğu ne kadar olmalı?

Anahtar uzunluğu hakkında bilgi verilen Tablo 2.3' de algoritma için yapılabilecek en iyi saldırının Kaba Kuvvet saldırısı olduğu varsayılmıştır. Büyük anahtar uzayı, algoritmanın güvenli olması için gereklidir ancak tek başına yeterli değildir. Şifre sisteminin aynı zamanda güçlü analitik ataklara karşı da dayanıklı olması gerekir.

Tablo 2.3. Kaba kuvvet saldırısının en başarılı olduğu bir algoritmada güvenliği sağlamak için yeterli anahtar uzunluğu (bit).

Anahtar uzunluğu	Güvenlik tahmini
56-64 bit	Kısa vadede: birkaç saat ya da gün güvenlidir
112-128 bit	Uzun vadede: Kuantum bilgisayarların olmadığı bir ortamda birkaç on yıl güvenlidir
256 bit	Uzun vadede: Kuantum bilgisayarlarla yapılan kuantum hesaplama algoritmalarına ragmen birkaç on yıl güvenlidir.

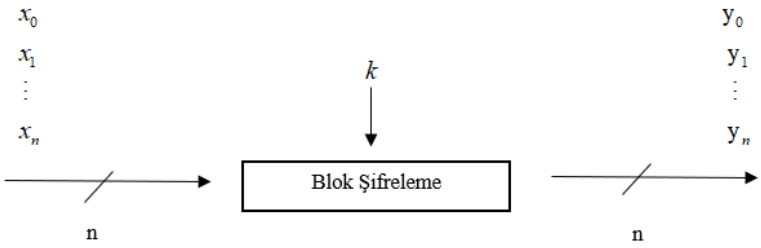
Simetrik Şifreleme, Blok Şifreleme ve Akış Şifreleme olmak üzere ikiye ayrılır.



Şekil 2.5. Simetrik şifreleme.

Blok şifreleme

Blok Şifrelemenin genel görünümü Şekil 2.6'da gösterilmektedir. Blok şifrelemeler,



Şekil 2.6. Blok şifrelemede işlem.

açık metnin blokları üzerinde işlem yapar ve şifreli metni bloklar halinde elde eder. Burada şifreleme ve deşifreleme işlemi $x, y \in \{0,1\}^n$ ve $k \in K$ anahtar olmak üzere,

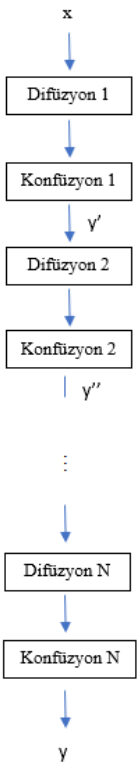
$$e_k(x) = y \tag{2.1}$$

$$d_k(y) = x \tag{2.2}$$

şeklinde yapılır. Blok şifrelemede açık metnin blok uzunluğu ile şifreli metnin blok uzunluğu eşit ve n bit olarak ifade edilir. Örneğin DES' te blok uzunluğu 64 bittir. Günümüzde modern blok şifrelemelerin büyük bir kısmı Claude Shannon' ın ürün şifresi (Product cipher) olarak adlandırdığı bir yöntemle inşa edilmiştir. Bu yönteme göre güçlü şifreleme algoritması üretmek için iki çeşit işlem vardır:

1. Karıştırma (Confusion): Şifreli metin ile anahtar arasındaki ilişkiyi gizlemek için yapılan şifreleme operasyonudur. Günümüzde bu işlem, AES ve DES' te de bulunan S-box (Substitution Box) ile yapılmaktadır.

2. Yayılma (Diffusion): Şifreleme aşamasında açık metnin özelliklerini gizlemek için açık metindeki bir karakterin şifreli metindeki birçok karakteri etkilemesi amaçlanır. Örneğin bit permütasyonu basit bir difüzyon işlemidir. DES' te difüzyon işlemi için bit permütasyonu, AES' te ise daha gelişmiş bir yöntem olan Mixcolumn işlemi kullanılır.

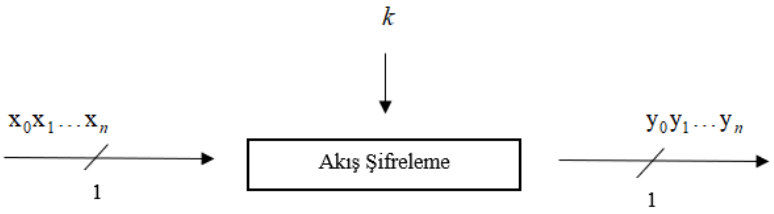


Şekil 2.7. N çevrimde ürün şifresi.

Shannon' a göre bu işlemleri Şekil 2.7.' deki gibi her çevrimde sırasıyla tekrarlayarak güçlü şifre sistemleri tasarlanabilir. Blok şifre sistemlerinden en bilinenleri DES ve AES' tir.

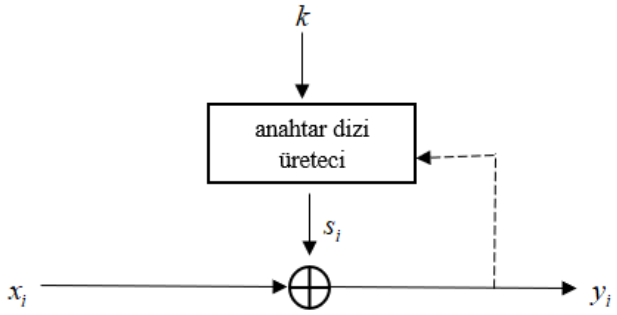
Akış şifreleme

Akış şifrelemesinde bitler tek tek şifrelenir. Bu işlem Şekil 2.8.' deki gibi anahtarın bir bitine açık metinden bir bitin eklenmesiyle yapılır.



Şekil 2.8. Akış şifrelemede işlem.

Anahtar dizisinin durumuna göre senkron akış şifreleme ve asenkron akış şifreleme olmak üzere iki farklı yöntem vardır. Senkron akış şifrelemesinde anahtar dizisi yalnızca anahtara bağlı iken asenkron akış şifrelemesinde anahtar dizisi hem anahtara hem de şifreli metne bağlıdır. Şekil 2.9.' da kesikli çizgi işlenirse asenkron akış şifrelemesi elde edilir.



Şekil 2.9. Senkron ve asenkron akış şifrelemesi.

Burada $x_i, y_i, s_i \in \{0,1\}$ sırasıyla açık metin, şifreli metin ve anahtar dizisi olmak üzere şifreleme ve deşifreleme işlemi sırasıyla

$$y_i = e_{s_i}(x_i) \equiv x_i + s_i \bmod 2 \tag{2.3}$$

$$x_i = d_{s_i}(y_i) \equiv y_i + s_i \bmod 2 \tag{2.4}$$

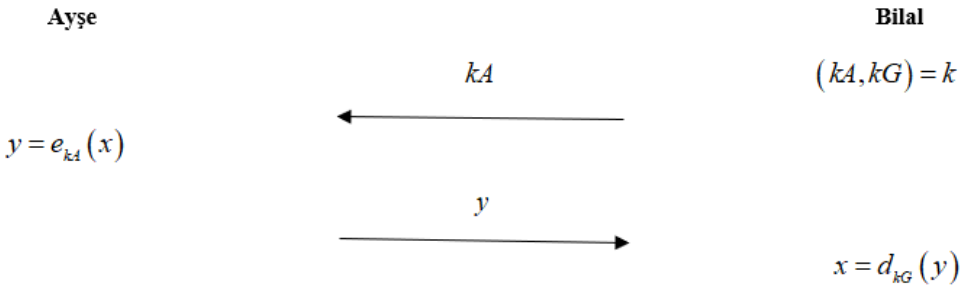
şeklindedir. Görüldüğü üzere şifreleme ve deşifreleme fonksiyonları oldukça basittir. Bu sebeple sistemin güvenliği tamamıyla $s_0, s_1, s_2, \ldots$ anahtar dizisine bağlıdır.

Sonuç olarak anahtar dizisinin rastgele olması yani bitler arası bağlantının tahmin edilemez olması büyük önem arz etmektedir. Akış şifrelemesindeki anahtar dizileri Rastgele Sayı Üreteçleri (Random Number Generator) ile elde edilmektedir.

2.2.1.2. Asimetrik şifreleme

Asimetrik şifreleme ya da Açık anahtarlı şifreleme olarak adlandırılan sistem 1976 yılında Diffie ve Hellman tarafından ortaya atılmıştır. 1977' de Rivest, Shamir ve Adleman tarafından asimetrik şifreleme tabanlı RSA kriptosistem tasarlanmıştır. Bu zamana kadar güvenliği çeşitli matematiksel problemlere dayanan birçok asimetrik şifreleme algoritması geliştirilmiştir.

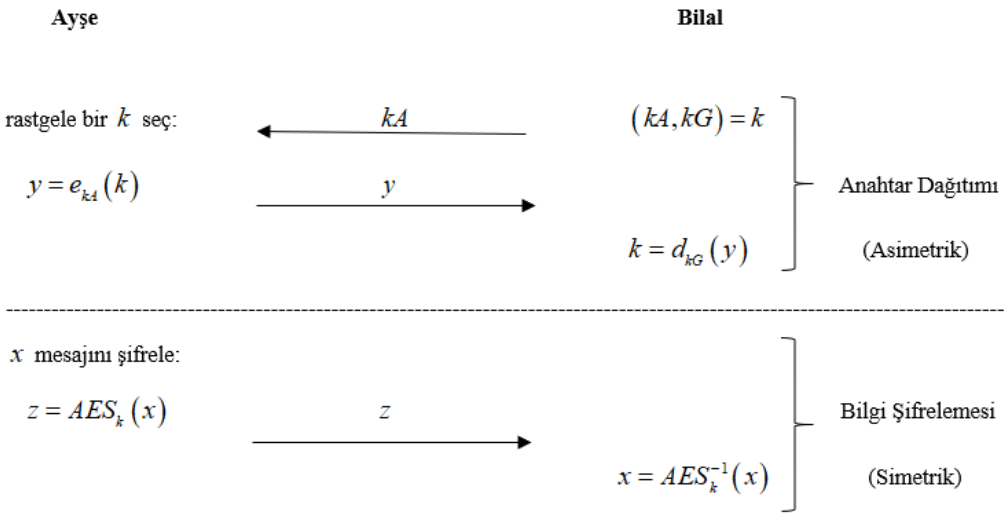
Asimetrik şifreleme ile simetrik şifreleme birbirinden oldukça farklıdır. Açık anahtarlı sistemlerde şifreleme fonksiyonu sayılar teorisi temelli çeşitli problemlere dayanırken simetrik sistemlerde açık metin ve şifreli metin çifti arasında bağ kurulamayacak şekilde her aşamada farklı fonksiyonlar kullanılır. Örneğin AES' in S-box kısmında kullanılan yöntem tüm sistem boyunca devam etmeyip yalnızca bu aşamada kullanılır.



Şekil 2.10. Asimetrik şifreleme.

Simetrik şifreleme sisteminde şifreleme ve deşifreleme aşamasında yalnız bir tane gizli anahtar kullanılırken açık anahtarlı sistemlerde gönderici ve alıcının birer gizli ve birer açık anahtarı vardır. Açık anahtar, herkesin görebileceği şekilde yayınlanırken gizli anahtar kullanıcıya özel olup gizlenir. Şekil 2.10.' da gösterildiği gibi sistemde gönderici pozisyonunda olan Ayşe, x mesajını alıcı pozisyonundaki Bilal' e iletmek istesin. İlk olarak Bilal kendi açık anahtarını güvensiz kanal üzerinden Ayşe' ye gönderir. Sonra Ayşe açık metni açık anahtar ile şifreleyip y şifreli metnini Bilal' e iletir. Son olarak, y şifreli metnini alan Bilal kendi gizli anahtarı ile deşifreleme yaparak x mesajını elde eder.

Açık anahtarlı şifreleme herhangi bir simetrik algoritmada güvensiz kanal üzerinden anahtar dağıtmak için de kullanılabilir. Asimetrik şifreleme ve simetrik şifrelemenin bir arada kullanıldığı sistemlere hibrit şifreleme sistemi denir. Örneğin Şekil 2.11.' deki gibi simetrik şifreleme algoritması olan AES' te kullanılacak olan anahtar asimetrik şifrelemeyle güvenli bir şekilde gönderici ve alıcı arasında dağıtılır.



Şekil 2.11. AES' te asimetrik şifreleme ile anahtar dağıtımı.

Sonuç olarak asimetrik şifreleme yüksek güvenlik gerektiren uygulamalar için iyi bir seçenektir. Açık anahtarlı sistemler tek yönlü fonksiyonlar kullanılarak inşa edilirler. Eğer,

1. $y = f(x)$ kolay hesaplanabilir, ve

2. $x = f^{-1}(y)$ hesaplaması imkansız

ise $f()$ fonksiyonuna tek yönlü fonksiyon denir. Tek yönlü fonksiyonlardan en popüler olanları tamsayılarda çarpanlara ayırma problemi, Ayrık Logaritma problemi ve Eliptik Eğri' dir. İlk asimetrik şifreleme algoritmalarından biri olan RSA' da tamsayılarda çarpanlara ayırma problemi kullanılır. Şimdi anahtar dağıtımı için önemli olan Diffie-Hellman anahtar değişimi algoritmasından bahsedelim.

Diffie-Hellman anahtar değişim algoritması

Whitfield Diffie ve Martin Hellman tarafından 1976' da yayınlanmıştır. İki mucit güvensiz kanal üzerinden haberleşerek ortak bir gizli anahtar belirleyebilecekleri bir yöntem geliştirmiştir. Bu algoritma, Ayrık Logaritma problemini temel alarak yapılmıştır. Sistemin ana fikri p asal bir sayı olmak üzere $\mathbb{Z}_p^*$' da çarpanlara ayırma

$$k = \left(\alpha^x\right)^y = \left(\alpha^y\right)^x \mod p \tag{2.5}$$

ve değiştirilebilen üs alma problemine dayanan tek yönlü fonksiyondur. Ortak gizli anahtar belirlenmeden önce aşağıdaki adımlar takip edilir:

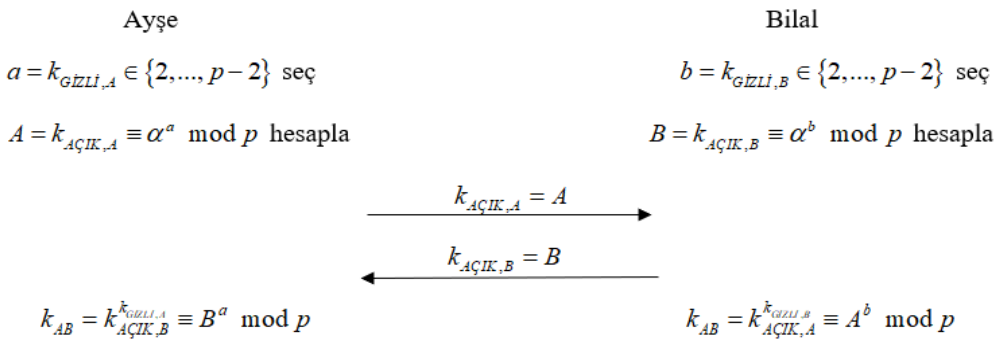
1. Çok büyük bir p asalı seçilir,
2. $\alpha \in \{2,3,...,p-2\}$ kümesinden bir tamsayı seçilir,
3. α ve p yayınlanır.

α ve p değerlerini bilen Ayşe ile Bilal Şekil 2.12.' deki adımları takip ederek ortak gizli anahtar k_{AB}'yi belirlerler. $k_{AB} \equiv \alpha^{ab} \mod p$ ortak anahtarı

$$B^a \equiv (\alpha^b)^a \equiv \alpha^{ab} \, mod \, p \tag{2.6}$$

$$A^b \equiv (\alpha^a)^b \equiv \alpha^{ab} \, mod \, p \tag{2.7}$$

işlemleri ile elde edilir.



Şekil 2.12. Diffie-Hellman anahtar dağıtımı.

Asimetrik algoritmalarda anahtar uzunluğu ne kadar olmalı?

Asimetrik algoritmalarda yeterli güvenliği sağlamak için gereken anahtar uzunluğu simetrik algoritmalara göre oldukça fazladır. Anahtar uzunluğu ne kadar fazla ise sistemin güvenlik düzeyi de o kadar yüksektir. Algoritmalar kıyaslanırken sağladıkları güvenlik seviyeleri göz önüne alınır. Eğer algoritmaya en iyi bilinen bir atağı yapmak için 2^n adım gerekiyorsa, algoritma "n bit güvenlik sağlar" denir. Simetrik algoritmalarda n bit anahtar uzunluğu olan bir sistem için n bit güvenlik sağlar denir. Tablo 2.4.' te asimetrik algoritmalarda 80,128,192 ve 256 bit güvenlik seviyeleri için gereken bit sayıları verilmiştir.

Tablo 2.4. Asimetrik algoritmalarda farklı güvenlik seviyeleri için gereken anahtar uzunluğu (bit).

Algoritma ailesi	Kriptosistemler	Güvenlik Seviyesi(bit)			
		80	128	192	256
Tamsayılarda çarpanlara ayırma	RSA	1024 bit	3072 bit	7680 bit	15360 bit
Ayrık Logaritma	DH, DSA, Elgamal	1024 bit	3072 bit	7680 bit	15360 bit
Eliptik Eğri	ECDH, ECDSA	160 bit	256 bit	384 bit	512 bit
Simetrik şifreleme	AES, 3DES	80 bit	128 bit	192 bit	256 bit

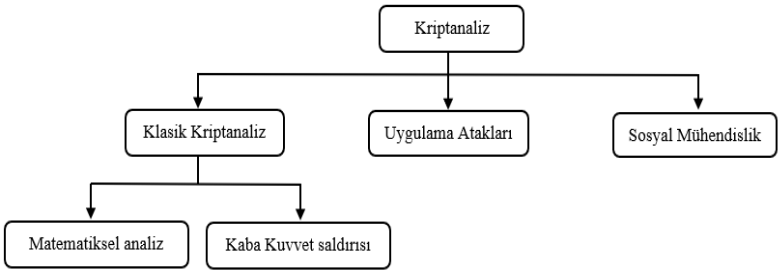
Uzun süreli güvenliği sağlamak için (birkaç on yıllık zaman dilimi), anahtar boyu 128 bit olarak seçilmelidir. Asimetrik şifrelemede büyük miktarlarda bit sayıları kullanılmasının bir sonucu olarak Dijital imzalama gibi bir işlemi yapmak, AES veya 3DES' te bir bloğu şifrelemek için gereken süreden 2-3 kat daha yavaştır. Örneğin RSA' da bir hesaplamada bit uzunluğunu 1024' ten 3076' ya çıkarmak ile hesaplama $3^3 = 27$ kat daha yavaş olacaktır.

2.2.1.3. Protokoller

Kabaca, kripto protokoller şifreleme algoritmalarının uygulanmasıyla ilgilenir. Bir protokol, algoritmaların nasıl kullanılması gerektiğini açıklar ve bir programın birden çok, birlikte çalışabilir sürümünü uygulamak için kullanılabileceği veri yapıları ve

gösterimleri hakkında ayrıntıları içerir. Simetrik ve asimetrik algoritmalar, güvenli internet iletişimi gibi uygulamaların gerçekleştirilebileceği yapı taşları olarak görülebilir. Örneğin bir kriptografi protokolü olan TLS (Transport Layer Security) yani taşıma katmanı güvenliği her tarayıcıda kullanılır.

2.2.2. Kriptanaliz



Şekil 2.13. Kriptanaliz' in yapısı.

Kriptanaliz: Kripto sistemleri kırmaya yönelik saldırıları inceleyen bilim dalıdır. Yeni bir sistem tasarlandığında oluşturulan yapının güvenilirlik seviyesini tespit etmek için çeşitli saldırı yöntemleri kullanılarak sistem kırılmaya çalışılır. Kriptanaliz' de kullanılan yöntemlerde genel hedef şifreyi kırıp anahtarı elde etmektir. Şifre kırmak için geliştirilmiş çeşitli yöntemler vardır. Şekil 2. 13.' de gösterildiği gibi Kriptanaliz, Klasik Kriptanaliz, Uygulama Atakları ve Sosyal Mühendislik olmak üzere üçe ayrılır. Bu başlıkta kriptanaliz yöntemleri hakkında bilgi verilecektir. Bu bölüm [32,34,37] kaynakları referans alınarak hazırlanmıştır.

2.2.2.1. Klasik kriptanaliz

Klasik Kriptanaliz, y şifreli metninden x açık metnini elde etme ya da y şifreli metninden k anahtarını elde etme bilimi olarak bilinir. Kriptanaliz, şifreleme algoritmasının iç yapısından faydalanarak yapılan analitik ataklar ve şifreleme algoritmasına bir kara kutu olarak bakıp, olası her anahtarı tek tek deneyerek yapılan Kaba Kuvvet saldırısı şeklinde ikiye ayrılır.

Kaba kuvvet saldırısı

Genellikle standart bilinen-şifreli metin ya da bilinen-açık metin saldırısı' na basitçe Kaba Kuvvet saldırısı denir. Saldırıda gelişmiş matematiksel işlemler ya da basitleştirme işlemi kullanılmadığı için bu şekilde adlandırılır. Bu yönteme göre

saldırgan, kanalı gizli dinleme yöntemiyle şifrelenmiş metni elde eder ve örneğin şifrelenmiş bir dosyanın adı gibi kısa bir açık metin parçası ele geçirir. Saldırgan ele geçirdiği bir miktar şifreli metni tüm olası anahtarlarla deşifreler. Eğer elde edilen açık metin, ele geçirilen açık metin ile eşleşiyorsa anahtar doğru olarak kabul edilir.

Tanım 2.2.2. Kaba Kuvvet saldırısı,

(x, y) Açık metin-şifreli metin çifti ve k_i, olası tüm anahtarların bulunduğu $K = \{k_1, ..., k_K\}$ anahtar uzayından bir anahtar olsun. Kaba Kuvvet saldırısında her $k_i \in K$ için

$$d_{k_i}(y) \stackrel{?}{=} x \tag{2.8}$$

eşitliğinin sağlanıp sağlanmadığı kontrol edilir. Eğer eşitlik doğru ise doğru anahtar bulunmuştur, değilse diğer anahtar için eşitliğin sağlanıp sağlanmadığı tekrar kontrol edilir.

Prensip olarak simetrik algoritmalar için Kaba Kuvvet saldırısının her zaman mümkün olduğu söylenebilir. Saldırının kolay uygulanabilir olup olmadığı ise anahtar uzayı ile ilişkilidir. Anahtar boyu küçük olan algoritmalar için Kaba Kuvvet saldırısı ile gizli anahtarı bulma yöntemi gayet uygundur. Örneğin anahtar boyu 40 bit olan bir şifreyi bir günde çözmeye çalışalım. Anahtar uzayında bulunan $2^{40} = 1,099,511,627,776$ tane anahtarı bir günde bulunan $24 \text{ x } 60 \text{ x } 60 = 86,400$ saniye içinde bulabilmek için saniyede $12,725,829$ adet anahtar denenmelidir. Güçlü bir bilgisayar için saniyede $4,000,000$ AES şifrelemesi yapmak mümkündür. Bu durumda 40-bitlik bir sistemi kırmak için 3 bilgisayarı aynı anda çalıştırırsak bir gün içinde doğru anahtarı elde ederiz.

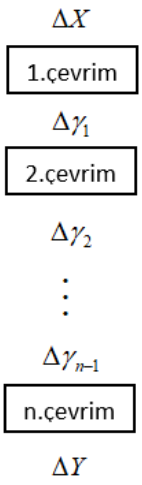
Matematiksel analiz

Bu bölümde simetrik blok şifre sistemlerine uygulanan oldukça güçlü iki atak yönteminden bahsedilecektir: Diferansiyel Kriptanaliz ve Lineer Kriptanaliz. Lineer Kriptanaliz Matsui tarafından geliştirilmiş ve ilk olarak DES üzerinde uygulanmıştır. Diferansiyel Kriptanaliz ise Biham ve Shamir tarafından geliştirilmiş ve ilk olarak DES' e uygulanmıştır. Bu ataklar ilk başta sadece DES' e uygulansa da, saldırıların

diğer blok şifrelere uygulanabilirliği çok kapsamlı olduğundan blok şifrelerin güvenlik seviyesini değerlendirme konusunda bu ataklar büyük öneme sahiptir.

Diferansiyel kriptanaliz

Diferansiyel Kriptanaliz, yüksek olasılığa sahip bir miktar açık metin farkları ve son çevrimin girdi farkları kullanılarak yapılır. Örneğin bir sistemde girdilerin kümesi $X = [X_1\ X_2\ \ldots X_n]$ ve çıktılarının kümesi $Y = [Y_1\ Y_2\ \ldots\ Y_n]$ olsun. Sistemin iki girdisi X' ve X'' ve buna karşılık gelen çıktılar sırasıyla Y' ile Y'' olsun. Burada $\oplus$ işlemi XOR yani özel-OR toplama işlemi olup $\bmod 2$ 'de toplama işlemini temsil eder. O halde sistemde girdi farkı $\Delta X = X' \oplus X''$ ve çıktı farkı $\Delta Y = Y' \oplus Y''$ şeklindedir. $(\Delta X, \Delta Y)$ çiftine bir diferansiyel denir. Diferansiyel Kriptanaliz bir çeşit seçilmiş-açık metin saldırısıdır. Yani saldırgan, anahtarı bulmak için açık metinleri seçer ve şifreli metinleri inceler. Diferansiyel karakteristik, çevrimlerin olasılık değeri yüksek girdi ve çıktı farklarından oluşan bir dizidir ve bir çevrimin çıktı farkı bir sonraki çevrimin girdi farkıdır.



Şekil 2.14. Diferansiyel karakteristik.

Yani her çevrim için bulunan fark dizisine diferansiyel karakteristik denir. Diferansiyel karakteristiğin gerçekleşme olasılığı ise her bir geçişin olasılığının çarpımı sonucu elde edilir.

$$(\Delta X, \Delta\gamma_1, \Delta\gamma_2, \ldots, \Delta\gamma_{n-1}, \Delta Y) \tag{2.9}$$

$$\Pr[\Delta X \to \Delta Y] = \Pr[\Delta X \to \Delta\gamma_1] \times \Pr[\Delta\gamma_1 \to \Delta\gamma_2] \times \bullet\bullet\bullet \times \Pr[\Delta\gamma_{n-1} \to \Delta Y] \tag{2.10}$$

Olasılık değeri yüksek bir diferansiyel karakteristik bulmak, son çevrimdeki bilgiyi kullanarak çevrim anahtarını ele geçirme imkanı verir. Diferansiyel Kriptanaliz'de diferansiyel karakteristiğin tamamını elde etmek için şifrenin S-box katmanının özellikleri incelenir ve bu özellikler kullanılır. Bu özelliklerden S-box katmanının girdi ve çıktı farkları kullanılarak yüksek olasılığa sahip fark çifti bulunur.

Diferansiyel dağılım tablosu

Şimdi S-box' ın $(\Delta X, \Delta Y)$ fark çiftlerini inceleyelim. Tablo 2.5.' te verilen 4x4 S-box için, girdi olarak $X = [X_1\ X_2\ X_3\ X_4]$ ve çıktı olarak $Y = [Y_1\ Y_2\ Y_3\ Y_4]$ alalım.

Tablo 2.5. S-box gösterimi (hexadecimal gösterim) [37].

Girdi	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
Çıktı	E	4	D	1	2	F	B	8	3	A	6	C	5	9	0	7

Her $(X', X'' = X' \oplus \Delta X)$ girdi çifti için ΔY değerini hesaplayarak Diferansiyel Dağılım Tablosu yapılır. Örneğin, Tablo 2.6.' da ikilik değerde olan X, Y ve değerleri 1011 (hex B), 1000 (hex 8) ve 0100 (hex 4) olan ΔX kullanılarak $(X, X \oplus \Delta X)$ girdi farkı için ΔY değerleri hesaplanmıştır. Tablodan görülebildiği gibi $\Delta X = 1011$ için karşılık gelen 16 değerden 8'i $\Delta Y = 0010$ değeridir (yani olasılık değeri $8/16$ dır.) Aynı şekilde $\Delta X = 1000$ için karşılık gelen 16 değerden 4' ü $\Delta Y = 1011$ dir.

Tablo 2.6. S-box' ın fark çiftleri [37].

X	Y	ΔY		
		$\Delta X = 1011$	$\Delta X = 1000$	$\Delta X = 0100$
0000	1110	0010	1101	1100
0001	0100	0010	1110	1011
0010	1101	0111	0101	0110
0011	0001	0010	1011	1001
0100	0010	0101	0111	1100
0101	1111	1111	0110	1011
0110	1011	0010	1011	0110
0111	1000	1101	1111	1001
1000	0011	0010	1101	0110
1001	1010	0111	1110	0011
1010	0110	0010	0101	0110
1011	1100	0010	1011	1011
1100	0101	1101	0111	0110
1101	1001	0010	0110	0011
1110	0000	1111	1011	0110
1111	0111	0101	1111	1011

$\Delta X = 0100$ için karşılık gelen 16 değerden 0' ı $\Delta Y = 1010$ ' dur. Bu şekilde her ΔX değeri için ΔY değeri hesaplanarak Diferansiyel Dağılım Tablosu yapılır. Bu işlemlerin tamamlanması ile elde edilen Tablo 2.7.' deki Diferansiyel dağılım tablosu' nun satırları ΔX değerlerini, sütunları ise ΔY değerlerinin ifade eder. Tablonun her hücresi satırda bulunan ΔX girdi farkı için bir ΔY çıktı farkının kaç defa bulunduğunu ifade eder.

Tablo 2.7. Diferansiyel dağılım tablosu [37].

		Output Difference															
		0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
Input Difference	0	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	1	0	0	0	2	0	0	0	2	0	2	4	0	4	2	0	0
	2	0	0	0	2	0	6	2	2	0	2	0	0	0	0	2	0
	3	0	0	2	0	2	0	0	0	0	4	2	0	2	0	0	4
	4	0	0	0	2	0	0	6	0	0	2	0	4	2	0	0	0
	5	0	4	0	0	0	2	2	0	0	0	4	0	2	0	0	2
	6	0	0	0	4	0	4	0	0	0	0	0	0	2	2	2	2
	7	0	0	2	2	2	0	2	0	0	2	2	0	0	0	0	4
	8	0	0	0	0	0	0	2	2	0	0	0	4	0	4	2	2
	9	0	2	0	0	2	0	0	4	2	0	2	2	2	0	0	0
	A	0	2	2	0	0	0	0	0	6	0	0	2	0	0	4	0
	B	0	0	8	0	0	2	0	2	0	0	0	0	0	2	0	2
	C	0	2	0	0	2	2	2	0	0	0	0	2	0	6	0	0
	D	0	4	0	0	0	0	0	4	2	0	2	0	2	0	2	0
	E	0	0	2	4	2	0	0	0	6	0	0	0	0	0	2	0
	F	0	2	0	0	6	0	0	0	0	4	0	2	0	0	2	0

Diferansiyel karakteristik inşası

SPN yapıdaki bir şifrenin S-box kısmı incelenerek elde edilen bilgi göz önüne alınarak tüm şifre için makul bir diferansiyel karakteristik bulunabilir. Bun işlem, S-box' ların uygun olan fark çiftleri bir araya getirilerek yapılabilir. Şekil 2.15.' te gösterildiği gibi $S_{12}, S_{23}, S_{32}, S_{33}$ içeren bir diferansiyel karakteristik inşa edelim. Şekilde fark değeri sıfırdan farklı olan S-box' lar koyu renk ile gösterilmiştir. Bu S-box' lar aktif S-box olarak adlandırılırlar. Aşağıdaki gibi S-box'ın fark çiftleri ile ilk 3 çevrim için diferansiyel karakteristik inşa edilecektir.

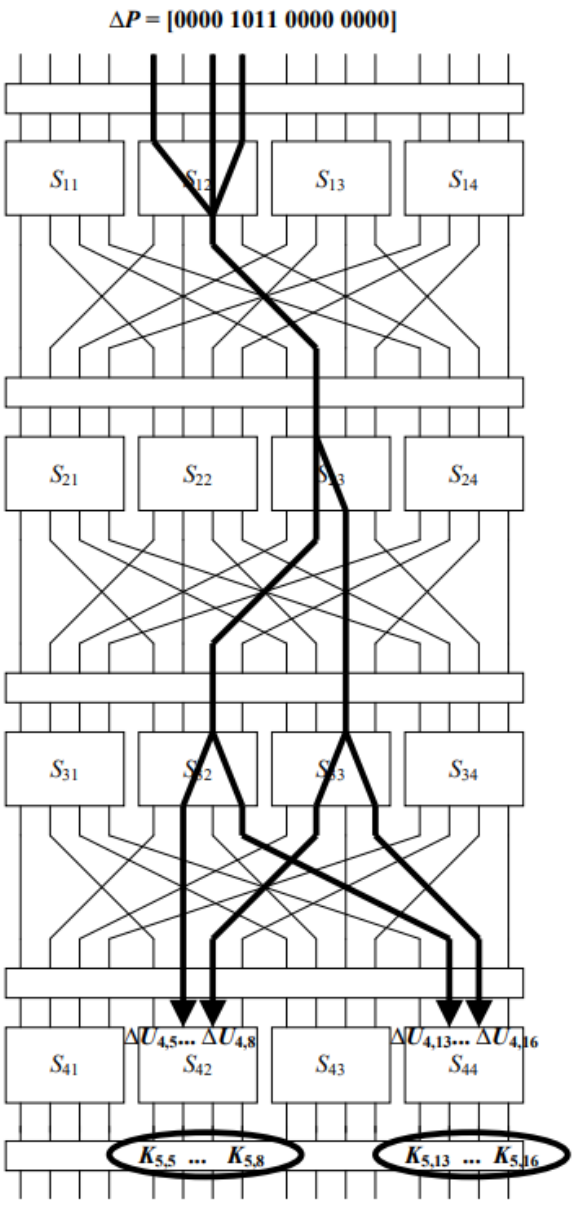
$$S_{12} : \Delta X = \mathrm{B} \rightarrow \Delta Y = 2 \quad \text{olasılık değeri } 8/16 \tag{2.11}$$

$$S_{23} : \Delta X = 4 \rightarrow \Delta Y = 6 \quad \text{olasılık değeri } 6/16 \tag{2.12}$$

$$S_{32} : \Delta X = 2 \rightarrow \Delta Y = 5 \quad \text{olasılık değeri } 6/16 \tag{2.13}$$

$$S_{32} : \Delta X = 2 \rightarrow \Delta Y = 5 \quad \text{olasılık değeri } 6/16 \tag{2.14}$$

Bu S-box' lar hariç diğerler S-box' lar girdi farkı sıfır olan ve dolayısıyla çıktı farkı sıfır olan S-box' lardır. Dolayısıyla aktif değildirler.



Şekil 2.15. Diferansiyel karakteristik örneği [37].

Bu karakteristiğin olasılık değeri $8/6\times6/16\times(6/16)^2 = 27/1024$ dir. Buradaki aktif S-box sayısı 4 tür.

Lineer kriptanaliz

Lineer Kriptanaliz, açık metin, şifreli metin ve çevrim anahtarı bitlerinden oluşan lineer ifadelerin yüksek olasılıklı olanlarını kullanarak saldırmayı hedefler. Bu atak,

bir çeşit bilinen-açık metin saldırısıdır: yani saldırgan, bir miktar açık metne ve bu açık metinlere karşılık gelen şifreli metinlere vakıftır. Saldırı, şifrenin bir kısmında kullanılan ve lineerliğin mod-2 ye göre bit bazında işlemi temsil ettiği bir lineer ifade kullanılarak yapılır. Böyle bir ifade, $X=[X_1, X_2, \ldots]$ girdisinin i. biti X_i ve $Y=[Y_1, Y_2, \ldots]$ çıktısının i. biti Y_i olmak üzere:

$$X_{i_1} \oplus X_{i_2} \oplus \ldots \oplus X_{i_u} \oplus Y_{j_1} \oplus Y_{j_2} \oplus \ldots \oplus Y_{j_v} = 0 \qquad (2.15)$$

şeklindedir. Burada $\oplus$ işlemi XOR yani özel-OR toplama işlemi olup $\mathrm{mod}\,2$ ' de toplama işlemini temsil eder. Bu saldırıda (2.15) deki gibi olasılık değeri çok yüksek ya da çok düşük olan ifadeler kullanılır. Eğer bir şifrede (2.15) deki gibi çok yüksek olasılıklı ya da çok düşük olasılıklı bir lineer ifade varsa şifrenin rastgelelik özelliğinin kötü olduğunu söyleyebiliriz (bir şifrenin kalitesi için kötü olan bir durum). Saldırganın elindeki lineer ifadenin olasılık değeri $1/2$ 'den ne kadar uzaksa Lineer Kriptanaliz' i yapmak o kadar elverişli olacaktır. Yani bir lineer yaklaşımın olasılığı $p_L > 1/2$ ya da $p_L < 1/2$ ise bu şifreye lineer atak yapmak uygundur. Bir lineer ifadenin olasılık değerinin $1/2$ ' den farkına yani $p_L - 1/2$ ifadesine lineer olasılık bias' ı denir. $|p_L - 1/2|$ ne kadar büyükse daha az bilinen-açık metin kullanarak Lineer Kriptanaliz yapmak o kadar kolaydır.

Lineer Kriptanaliz, şifrenin tek lineer-olmayan bölümü olan S-box' ın özellikleri kullanılarak yapılır. S-box' ın lineer olmayan özellikleri kullanılarak S-box'ın girdi kümesi ile çıktı kümesi arasında bir lineer yaklaşım oluşturulabilir. Dolayısı ile, S-box' ların lineer yaklaşımlarını birleştirdiğimizde aradaki bitler yok olur ve geriye sadece yüksek bias değerine sahip açık metin bitleri ve son çevrimin girdi bitleri kalır.

Tanım 2.2.3. Piling – Up Lemma (Matsui 1)

n tane bağımsız, rastgele $X_1, X_2, \ldots, X_n$ değerleri için,

$$\Pr\left(X_1 \oplus \ldots \oplus X_n = 0\right) = 1/2 + 2^{n-1} \prod_{i=1}^{n} \varepsilon_i \qquad (2.16)$$

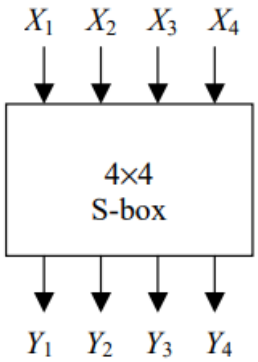
ya da, buna denk olarak, $X_1 \oplus \ldots \oplus X_n = 0$ ifadesinin bias'ı $\varepsilon_{1,2,\ldots,n}$ olmak üzere,

$$\varepsilon_{1,2,\ldots,n} = 2^{n-1} \prod_{i=1}^{n} \varepsilon_i \tag{2.17}$$

şeklindedir.

Lineer yaklaşım tablosu

Tablo 2.5.' deki S-box için girdi $X = [X_1\ X_2\ X_3\ X_4]$ ve buna karşılık gelen çıktı Şekil 2.16' daki gibi $Y = [Y_1\ Y_2\ Y_3\ Y_4]$ olsun. Her bir lineer yaklaşım için bias değeri hesaplanarak kullanıma uygun olup olmadığı belirlenir. Dolayısıyla, girdisi ve çıktısının sırasıyla X , Y olduğu bir S-box için (2.15) tipindeki tüm lineer yaklaşımlar incelenir.



Şekil 2.16. S-box fonksiyonu [37].

Örneğin, şifrede kullanılan Tablo 2.5.' teki S-box için $X_2 \oplus X_3 \oplus Y_1 \oplus Y_3 \oplus Y_4 = 0$ lineer yaklaşımı ya da bu ifadeye denk olan,

$$X_2 \oplus X_3 = Y_1 \oplus Y_3 \oplus Y_4 \tag{2.18}$$

ifadesini inceleyelim. X girdisi için bulunan tüm ihtimalleri deneyerek tüm Y çıktılarını inceleyerek, bu lineer yaklaşımın 16 durumdan 12' sinde doğru olduğunu görürüz. Dolayısıyla, bu ifadede olasılık $p_L = 12/16$ ve lineer olasılık bias' ı

$$p_L - 1/2 = 12/16 - 1/2 = 1/4 \tag{2.19}$$

dir. Tablo 2.8.' de bu durum gösterilmiştir. Benzer olarak,

$$X_1 \oplus X_4 = Y_2 \tag{2.20}$$

lineer yaklaşımı için olasılık değeri $p_L = 8/16$ ve lineer olasılık bias' ı $p_L - 1/2 = 0$ ' dır. Yine aynı şekilde

$$X_3 \oplus X_4 = Y_1 \oplus Y_4 \tag{2.21}$$

için olasılık değeri $p_L = 2/16$ ve lineer bias'ı $2/16 - 1/2 = -3/8$ şeklindedir.

Tablo 2.8. S-box' ın lineer yaklaşım örneği [37].

X_1	X_2	X_3	X_4	Y_1	Y_2	Y_3	Y_4	$X_2 \oplus X_3$	$Y_1 \oplus Y_3 \oplus Y_4$	$X_1 \oplus X_4$	Y_2	$X_3 \oplus X_4$	$Y_1 \oplus Y_4$
0	0	0	0	1	1	1	0	0	0	0	1	0	1
0	0	0	1	0	1	0	0	0	0	1	1	1	0
0	0	1	0	1	1	0	1	1	0	0	1	1	0
0	0	1	1	0	0	0	1	1	1	1	0	0	1
0	1	0	0	0	0	1	0	1	1	0	0	0	0
0	1	0	1	1	1	1	1	1	1	1	1	1	0
0	1	1	0	1	0	1	1	0	1	0	0	1	0
0	1	1	1	1	0	0	0	0	1	1	0	0	1
1	0	0	0	0	0	1	1	0	0	1	0	0	1
1	0	0	1	1	0	1	0	0	0	0	0	1	1
1	0	1	0	0	1	1	0	1	1	1	1	1	0
1	0	1	1	1	1	0	0	1	1	0	1	0	1
1	1	0	0	0	1	0	1	1	1	1	1	0	1
1	1	0	1	1	0	0	1	1	0	0	0	1	0
1	1	1	0	0	0	0	0	0	0	1	0	1	0
1	1	1	1	0	1	1	1	0	0	0	1	0	1

Bu şekilde her lineer yaklaşım için bir bias hesabı yapıldığında Tablo 2.9.' daki gibi bir lineer yaklaşım tablosu elde edilir. Tablodaki her eleman bir lineer yaklaşımda girdi toplamı ile çıktı toplamının kaç defa eşleştiğini ifade eder. Yani tablodaki herhangi bir hücredeki değeri 16' ya bölmek suretiyle (karşılık geldiği girdi toplamı ve çıktı toplamı ile temsil edilen) lineer yaklaşımın lineer olasılık bias' ı elde edilir.

Tablo 2.9. Lineer yaklaşım tablosu [37].

		Output Sum															
		0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
Input Sum	0	+8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	1	0	0	−2	−2	0	0	−2	+6	+2	+2	0	0	+2	+2	0	0
	2	0	0	−2	−2	0	0	−2	−2	0	0	+2	+2	0	0	−6	+2
	3	0	0	0	0	0	0	0	0	+2	−6	−2	−2	+2	+2	−2	−2
	4	0	+2	0	−2	−2	−4	−2	0	0	−2	0	+2	+2	−4	+2	0
	5	0	−2	−2	0	−2	0	+4	+2	−2	0	−4	+2	0	−2	−2	0
	6	0	+2	−2	+4	+2	0	0	+2	0	−2	+2	+4	−2	0	0	−2
	7	0	−2	0	+2	+2	−4	+2	0	−2	0	+2	0	+4	+2	0	+2
	8	0	0	0	0	0	0	0	0	−2	+2	+2	−2	+2	−2	−2	−6
	9	0	0	−2	−2	0	0	−2	−2	−4	0	−2	+2	0	+4	+2	−2
	A	0	+4	−2	+2	−4	0	+2	−2	+2	+2	0	0	+2	+2	0	0
	B	0	+4	0	−4	+4	0	+4	0	0	0	0	0	0	0	0	0
	C	0	−2	+4	−2	−2	0	+2	0	+2	0	+2	+4	0	+2	0	−2
	D	0	+2	+2	0	−2	+4	0	+2	−4	−2	+2	0	+2	0	0	+2
	E	0	+2	+2	0	−2	−4	0	+2	−2	0	0	−2	−4	+2	−2	0
	F	0	−2	−4	−2	−2	0	+2	0	0	−2	+4	−2	−2	0	+2	0

$a_i \in \{0,1\}$ ve "." İşleminin AND operasyonu olduğu bir ortamda girdi değişkenlerinin bir lineer kombinasyonu, $a_1X_1 \oplus a_2X_2 \oplus a_3X_3 \oplus a_4X_4$ olsun. O halde bu ifadenin onaltılık (hexadecimal) gösterimi, a_1 MSB (Most Significant Bit) olmak üzere, $a_1a_2a_3a_4$ ikilik değeri (binary value) ile ifade edilir. Aynı şekilde $b_i \in \{0,1\}$ için lineer kombinasyonu $b_1Y_1 \oplus b_2Y_2 \oplus b_3Y_3 \oplus b_4Y_4$ olan çıktı değişkenlerinin onaltılık gösterimi, $b_1b_2b_3b_4$ ikilik değeri ile gösterilir. Örneğin,

$$X_3 \oplus X_4 = Y_1 \oplus Y_4 \tag{2.22}$$

lineer denklemi için (onaltılık girdi değeri: 3 ve onaltılık çıktı değeri: 9) bias değeri $-6/16 = -3/8$ ve lineer olasılığı $1/2 - 3/8 = 1/8$ dir.

Lineer Yaklaşım İnşası

SPN bir yapıda S-box incelenerek elde edilen lineer yaklaşım tablosu olan Tablo 2.9. ile tüm şifre için lineer yaklaşımlar belirlenebilir. Bu işlem, S-box' ların uygun lineer yaklaşımları birleştirilmek suretiyle yapılır. Açık metin bitlerini ve sondan ikinci çevrimin S-box çıktısını içeren bir lineer yaklaşım ile son çevrimden çevrim anahtarını

elde ederek lineer saldırıyı yapmak mümkündür. Şekil 2.17.' de gösterildiği gibi $S_{12}, S_{22}, S_{32}, S_{34}$ içeren bir lineer yaklaşımı ele alalım. Bu yaklaşımın yalnızca ilk 3 çevrimi içerdiğini unutmayalım. S-box' lar için aşağıdaki lineer yaklaşımları kullanalım:

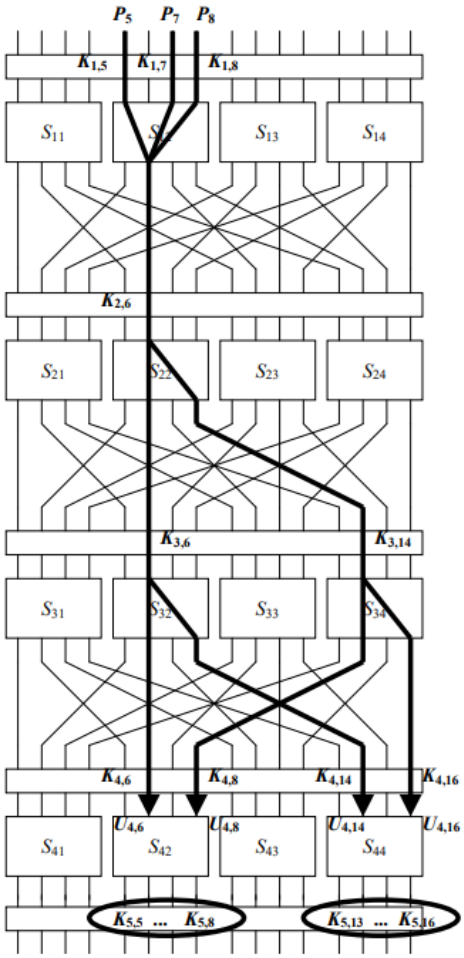
$$S_{12} : X_1 \oplus X_3 \oplus X_4 = Y_2 \text{ için olasılık } 12/16 \text{ ve bias değeri } +4/16 \text{ dır} \quad (2.23)$$

$$S_{22} : X_2 = Y_2 \oplus Y_4 \text{ için olasılık } 4/16 \text{ ve bias değeri } -4/16 \text{ dır} \quad (2.24)$$

$$S_{32} : X_2 = Y_2 \oplus Y_4 \text{ için olasılık } 4/16 \text{ ve bias değeri } -4/16 \text{ dır} \quad (2.25)$$

$$S_{34} : X_2 = Y_2 \oplus Y_4 \text{ için olasılık } 4/16 \text{ ve bias değeri } -4/16 \text{ dır} \quad (2.26)$$

Burada ilk 3 çevrim için aktif S-box sayısı 4' tür.



Şekil 2.17. Lineer Yaklaşım örneği [37].

2.2.2.2. Uygulama atakları

Yan kanal analizi, örneğin gizli anahtar kısmı için çalışan işlemcinin elektriksel güç tüketimini ölçerek gizli anahtarı elde etmek için kullanılır. O halde güç tüketimi sinyal işleme teknikleri uygulanarak anahtarı ele geçirmek için kullanılabilir. Güç tüketiminin yanı sıra elektromanyetik radyasyon ya da programın işlenme süresi (runtime) de gizli anahtar hakkında birtakım bilgiler elde etmemizi sağlar. Ancak uygulama atakları yalnızca saldırganın akıllı kartlar gibi doğrudan sisteme erişimi olması durumunda kriptosistemler için tehlike arz etmektedir. Dolayısıyla uygulama atakları, uzaktan erişimli sistemlere karşı yapılan internet tabanlı saldırıların çoğunda tehdit olarak görülmemektedir.

2.2.2.3. Sosyal mühendislik atakları

İnsanlar üzerinde rüşvet verme, şantaj, dolandırma ya da klasik casusluk yöntemleri uygulamak suretiyle anahtarı ele geçirme yöntemine "Sosyal Mühendislik Atakları" denir. Örneğin bir kişinin başına silah dayamak suretiyle anahtarı söylemesi için zorlamak bir çeşit sosyal mühendisliktir. Ya da insanları telefon ile arayarak "Şirketinizin bilgi işlem departmanından aranıyorsunuz. Yazılım güncellemesi için şifrenize ihtiyacımız var." şeklinde bir dolandırıcılık yöntemi de buna bir örnektir.

Saldırılar hakkında bazı bilgiler elde ettikten sonra kriptosistemler hakkında bilmemiz gereken en önemli unsur, saldırganlar her zaman sistemin en zayıf olduğu kısma odaklanırlar. Bu sebeple sistemimiz için güçlü algoritmalar seçmeli ve sosyal mühendislik ile uygulama ataklarının imkansız olduğundan emin olmalıyız.

Bir kriptosistem, saldırganın sistemin içeriği hakkında ayrıntılı bilgiye sahip olması durumunda bile güvenli olmalıdır. Dayanıklı bir kriptosistem yapmak için 1883' te Auguste Kerckhoffs tarafından ortaya atılan Kerckhoffs Prensibi' ne bağlı kalınmalıdır. Bu prensibe göre: bir kriptosistem, saldırganın gizli anahtar hariç sistemdeki her ayrıntıyı bilmesine rağmen güvenli kalmalıdır. Özellikle saldırganın şifreleme ve deşifreleme algoritmalarını bilmesi durumunda dahi sistem güvenli olmalıdır.

2.3. DNA Şifreleme

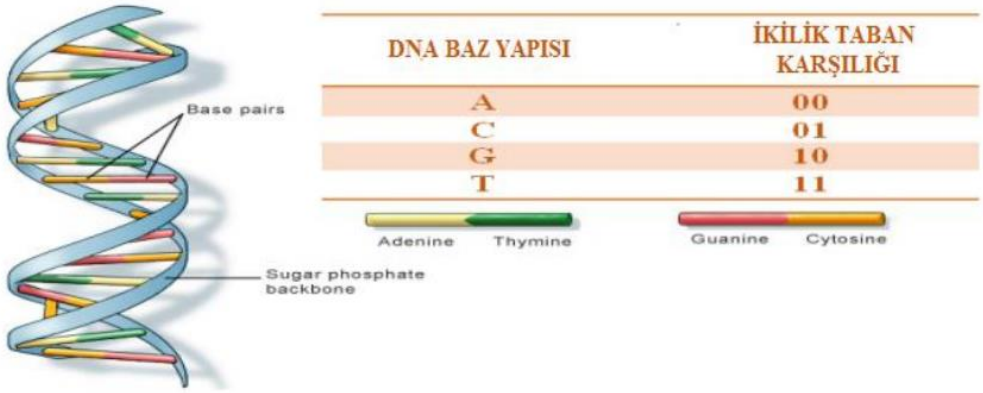
DNA tabanlı şifreleme yine güçlü kriptografik algoritmaların temelinde kullanılmaktadır. Buna göre bir algoritmada bir biyomoleküler teknik olan DNA hesaplama yöntemi kullanılarak güçlü ve güvenli algoritmalar tasarlamak mümkündür. DNA hesaplama yöntemi, Adleman tarafından geliştirilmiş bir yöntemdir. Bu yöntem ile kriptografi ve bazı biyomoleküler kavramlar bir arada kullanılarak yeni bir yaklaşım geliştirilmiştir [38].

Teknik olarak DNA yapısının bu alanda kullanılmasının birçok nedeni vardır. Buna göre bir gram DNA'da yaklaşık olarak 10^6 TB'lık bir depolama alanı mevcuttur. Dolayısıyla birkaç gram DNA ile dünyadaki tüm verilerin depolanabileceği bir ortam elde edilebilir. Diğer bir özellik olarak DNA'nın karmaşık yapısı sayesinde, içeriğinde saklanan bilgiler güvenli bir şekilde korunabilir [38].

2.3.1. DNA yapısı

DNA, canlıların hücrelerinde bulunan ve genetik özelliklerini taşıyan bir moleküldür. DNA'nın yapı taşı nükleotittir. Nükleotitler, azotlu baz, beş karbon şeker ve bir fosfat grubundan oluşur. Azotlu bazın ise dört çeşidi vardır. Bunlar Adenin (A), Guanin (G), Sitozin (C) ve Timin (T) şeklindedir. DNA'nın bir iplikçiği, bu dört bazın, yapısı şeker ve fosfattan oluşan bir iskete tutunması ile elde edilir [38]. DNA zinciri iki iplikçikten oluşur ve bu iplikçikler birbirine WCC (Watson Crick complement) tekniğine göre bağlanırlar. Bu tekniğe göre A ile T ve G ile C birbirini tamamlar ve $A^C = T$ ve $G^C = C$ ile ifade edilirler. DNA çift sarmalında A ile T ikili hidrojen bağı ve C ile G üçlü hidrojen bağı kurarlar [39].

DNA steganografisi bir kriptografi tekniği olarak 2. Dünya savaşından bu yana kullanılmaktadır. DNA steganografisi yöntemi DNA kodlu bir mesajın bir DNA örneği içerisine gizlenmesidir.



Şekil 2.18. DNA dijital kodlaması [38].

DNA kodlama, bir düz metni DNA zincirine dönüştürme işlemidir. Öncelikle düz metindeki karakterlerin ASCII tablosuna göre ikilik tabana karşılık gelen değerleri elde edilir. Ardından her ikili değeri baza dönüştürme işlemi yapılır. Şekil 2. 18 de gösterildiği gibi A bazı 00, C bazı 01, G bazı 10 ve T bazı 11 ile eşleştirilmiştir. Örneğin, iki harften oluşan FB metnini DNA kodlama yöntemine göre yazarsak,

$$\begin{array}{c} \text{FB} \\ \downarrow \\ \text{ASCII} \\ \downarrow \\ 0100011001000010 \\ \downarrow \\ \text{CACGCAAG} \end{array} \tag{2.27}$$

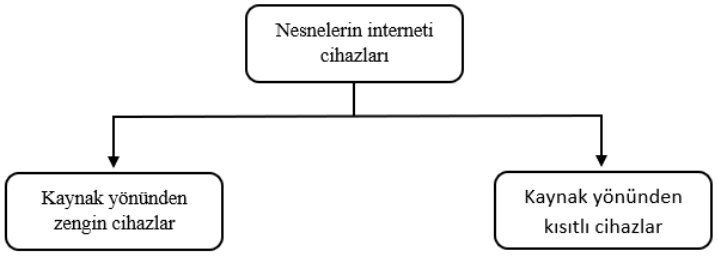
Metnin son hali CACGCAAG olarak elde edilir. DNA çift sarmalını oluşturan yapıda iki iplikçik bulunmaktadır. Bu ipliklerden ilki 5'-ucundan 3'-ucuna doğru yazılır ve çift sarmallı yapı oluşturulurken 3'-ucu ve 5'-ucu birbirini tamamlar. Örneğin, WCC kuralına göre $5' - AGCCGTAGCT - 3'$ ile $5' - AGCTACGGCT - 3'$ dizileri birbirine bağlanarak DNA çift zincirini oluşturur.

3. HAFİF KRİPTOGRAFİ (LIGHTWEIGHT CRYPTOGRAPHY)

3.1. Nesnelerin İnterneti

Son zamanlarda Nesnelerin İnterneti' nin (IOT) birçok uygulamasının insan hayatının çeşitli alanlarında yaygın olarak kullanıldığını görmekteyiz. Akıllı evler, giyilebilir teknolojiler, endüstriyel akıllı izleme sistemleri Nesnelerin İnternetine birer örnektir. Nesnelerin İnterneti terim olarak ilk defa bir RFID (Radyo Frekansı ile Tanımlama teknolojisi) projesinde 1999 yılında Kevin Ashton tarafından kullanılmıştır. 2009' da Nesnelerin İnterneti terimi kablolu veya kablosuz olarak birbirine bağlanabilen birbiriyle ilişkili bir grup cihaz anlamında kullanıldığından beri teknoloji, altyapı ve IOT kullanımı büyük oranda gelişmiştir [40].

Nesnelerin İnterneti, internet üzerinden insan etkileşimi olarak ya da olmayarak bilgi toplayan ya da değiştiren farklı özelliklere sahip birçok cihazın birbiriyle etkileşimini sağlayan bir ağdır. Herhangi bir Nesnelerin İnterneti uygulaması ya da çözümünde Nesnelerin İnterneti cihazları en temel unsurlardır. Nesnelerin İnterneti cihazları Şekil 3.1' deki gibi iki kategoriye ayrılabilir: server' lar, bilgisayarlar, tabletler ve akıllı telefonlar vb. gibi kaynak yönünden zengin olan cihazlar ve sensörler, sensör düğümleri, RFID (Radyo frekansı ile tanımlama teknolojisi), kumanda vb. gibi kaynak yönünden kısıtlı olan cihazlar [3].



Şekil 3.1. İki kategoriye ayrılabilen nesnelerin interneti cihazları.

İkinci kategoriye giren cihazlar, çeşitli alanlarda yaygın olarak kullanıldığı ve piyasayı oluşturan cihazların çoğunu oluşturduğu için daha popülerdir.

Milyonlarca akıllı cihazın etkileşim halinde çalıştığı ortamlarda, özellikle server'lardan sensörlere bilgi aktarırken cihazlarda kullanıcılar için çeşitli güvenlik ve gizlilik problemleri ortaya çıkmaktadır. Aynı zamanda Nesnelerin İnterneti cihazları kolay ulaşılabilir ve saldırılara karşı dayanıksızdır çünkü kişisel verileri toplamak ya da fiziksel çevre değişkenlerini kontrol etmek için doğrudan dış dünya ile etkileşimde bulunurlar ki bu da saldırganlar için bu cihazları cazip bir hedef haline getirir. Tüm bu şartlar Nesnelerin İnterneti cihazlarında siber güvenliği ve bunun yanı sıra gizlilik, kimlik doğrulama ve yetkilendirme, ulaşılabilirlik, mahremiyet ve düzenleme standartlarını önemli kılar. Bu durumda kriptografi güzel bir çözüm sunar. Ancak geleneksel bilgisayar tabanlı kriptografi uygulamaları kısıtlı kaynağa sahip cihazlar için uygun değildir. Bu tarz uygulamaların daha hafif hali olan Hafif Kriptografi, kaynak yönünden kısıtlı Nesnelerin İnterneti cihazlarında güvenli haberleşme için kullanılabilir.

Nesnelerin İnterneti cihazlarına geleneksel kriptografiyi uygularken karşılaşılan zorluklar:

1) Sınırlı hafıza (RAM, ROM)
2) Azaltılmış bilgi işlem gücü
3) Montaj yapmak için ayrılmış alanın küçük olması
4) Düşük batarya gücü (ya da bataryasız olma durumu)
5) Gerçek zamanlı yanıt

Nesnelerin interneti cihazlarının çoğu küçük boyutlardadır ve uygulamayı saklamak veya çalıştırmak için küçük bir hafıza (RAM, ROM), bilgiyi üretmek için düşük hesaplama gücü, kısıtlı batarya gücü, montaj için küçük bir alanın ayrılması gibi kısıtlı kaynaklara sahiptir. Dolayısıyla bu cihazlara geleneksel kriptografi' nin uygulanması durumunda beklenen performans alınamaz. Yukarıda bahsedilen sorunların tamamı geleneksel kriptografi' nin bir alt dalı olan ve küçük hafıza, küçük işlem gücü, düşük enerji harcaması, gerçek zamanlı yanıt gibi hafif özelliklere sahip Hafif Kriptografi ile çözülebilmektedir. Hafif Kriptografi, geleneksel kriptografinin aksine hem kaynak

yönünden kısıtlı cihazlarda (sensörler, RFID etiketleri, vb.) hem de kaynak yönünden zengin olan cihazlarda (serverlar, bilgisayarlar, tabletler, akıllı telefonlar, vb.) kullanılabilmektedir.

3.2. Hafif Kriptografi

Nesnelerin İnterneti cihazlarında yukarıda bahsedilen zayıf hesaplama kabiliyeti, küçük depolama alanı ve kısıtlı enerji gibi özellikleri sebebiyle AES gibi geleneksel şifreleme teknikleri uygun değildir. Bu sebeple son yıllarda Hafif Kriptografi' ye olan ilgi artmıştır. Hafif Kriptografi'nin üç temel özelliği vardır. Birincisi kaynak kısıtlı cihazlarda büyük verilerden ziyade küçük veriler şifrelenir. Dolayısıyla bu şifreleme daha verimlidir. İkincisi bu şifreleme çeşidinde saldırganlar bilgi ve hesaplama kabiliyetinden yoksun olduğu için şifrenin daha düşük seviyede güvenliğe ihtiyacı vardır. Sonuncusu, Hafif Kriptografi genel olarak donanımda kullanılır ve çok küçük bir kısmı yazılım için kullanılır [18].

Hafif Kriptografi' nin nitelikleri ve bunlar için bazı öneriler Tablo 3.1'de verilmiştir. Buna göre kriptografiyi herhangi bir Nesnelerin İnterneti cihazına uyarlarken göz önüne alınması gereken nitelikler fiziksel maliyet, performans ve güvenliktir [3].

Tablo 3.1. Hafif kriptografinin nitelikleri.

	Nitelikler	Hafif Kriptografi'nin önerisi
Fiziksel (Maliyet)	Fiziksel alan (G'ler,…) Hafıza (RAM, ROM) Batarya gücü (tüketilen enerji)	Küçük anahtar ve blok Basit hesaplama kullanılan basit çevrimler
Performans	Hesaplama gücü mukavemeti (bit)	Basit anahtar üretimi
Güvenlik	En küçük güvenlik mukavemeti (bit) Saldırı modelleri (anahtar benzerliği,çoklu anahtar)	Güçlü iç yapı

Hafif algoritmalarda ilk iki nitelik basit anahtar şeması ile üretilen küçük boyutlu anahtarlar (≤ 80 bit) ve küçük bloklar (≤ 64 bit) kullanılarak oluşturulan basit çevrim fonksiyonu ile sağlanır. Sonuncu nitelik olan güvenlik için 6 iç yapı çeşidinden (SPN, FN, GFN, ARX, NLFSR, Hibrit) uygun olanı kullanılarak algoritmanın saldırılara karşı dirençli hale gelmesi hedeflenir.

3.2.1. Hafif kriptografi tasarım ölçütleri

3.2.1.1.Simetrik şifreleme ve asimetrik şifreleme

Kriptografik algoritmalar, simetrik algoritmalar ve asimetrik algoritmalar olmak üzere ikiye ayrılır. simetrik algoritmalar hem şifreleme hem de deşifreleme için aynı anahtarı kullanırken, asimetrik algoritmalar şifreleme ve deşifreleme için iki farklı anahtar kullanır. Simetrik algoritmalar güvenli ve asimetrik algoritmalara kıyasla çok daha hızlıdır. Ancak simetrik algoritmalarda tek problem taraflar arasında anahtar dağıtımını zafiyet vermeden güvenli olarak yapmaktır. Ancak anahtarı taraflar arasında güvenilir bir üçüncü taraf aracılığıyla dağıtarak problemi çözebiliriz. Bu şifreleme yöntemiyle bilginin gizliliği, veri bütünlüğü ve kimlik doğrulama yapılabilir. Asimetrik algoritmalar iki çeşit anahtar kullanır. Alıcının açık anahtarını kullanarak gizlilik ve bütünlük ilkeleri sağlanırken, deşifrelerken göndericinin gizli anahtarını kullanarak kimlik doğrulama ilkesi (dijital imza olarak) sağlanır. Asimetrik şifrelemenin tek dezavantajı çok büyük boyutlarda anahtar kullanması sebebiyle karmaşıklığı artırıp süreci yavaşlatmasıdır.

3.2.1.2. Blok şifreleme ve akış şifreleme

Blok şifrelemede hem şifreleme hem de deşifreleme aynı blok boyuna sahip (64 bit ya da daha fazla) bloklar üzerinde yapılırken akış şifrelemesinde bitler tek tek şifrelenir. Bir algoritmada, Claude Shannon teorisine göre şifreyi güçlendirmek için konfüzyon difüzyon özellikleri bulunmalıdır. Buna göre konfüzyon özelliği şifreli metin ile anahtar arasındaki bağlantıyı S-box kullanmak suretiyle karmaşık hale getirmeye çalışırken, difüzyonda permütasyon işlemi kullanarak açık metnin tüm özelliklerini şifreli metnin tamamına yaymak hedeflenir. Akış şifrelemesinde yalnızca konfüzyon

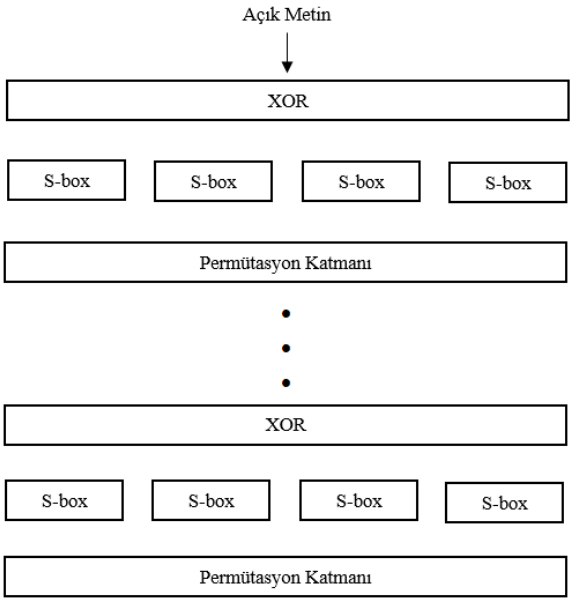
kullanılırken, blok şifrelemesinde daha basit bir tasarımla hem difüzyon hem de konfüzyon özellikleri kullanılır. Blok şifrelemesinde şifreleme işleminde tersten gidip açık metni elde etmek zor iken akış şifrelemesinde genelde XOR işlemi kullanılır ki bunun tersi yine XOR işlemi olduğundan açık metne ulaşmak daha kolaydır. Dolayısıyla kaynak kısıtlı Nesnelerin İnterneti cihazlarında güvenlik açısından akış şifrelemesi yerine blok şifreleme tercih edilir.

3.2.1.3. Simetrik blok şifre yapısı

Simetrik blok şifreleri yapısal olarak aşağıdaki gibi sınıflandırılır:

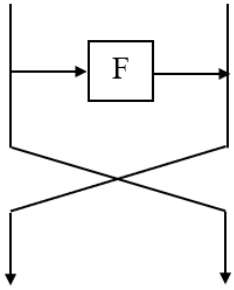
1) SPN yapı (Substitution-Permutation Network)
2) Feistel yapı
3) Genelleştirilmiş Feistel yapısı (General Feistel Network)
4) Topla-Kaydır-XOR yapısı (Add-Rotate-XOR)
5) Doğrusal Olmayan Bir Geri Bildirim Kaydırma Yazmacı (NLFSR)
6) Hibrit yapı

Şekil 3.2 deki gibi SPN yapısı veriyi S-box ve permütasyondan oluşan bir dizi işleme tabi tutarak bir sonraki çevrime hazırlar.



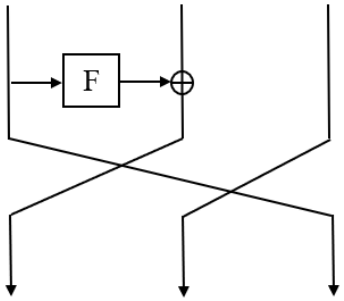
Şekil 3.2. SPN yapı.

Şekil 3.3'teki gibi Feistel yapıda (FN) çevrim girdisi iki eşit parçaya bölünür ve yalnızca parçanın bir yarısı SPN yapıya sahip olan F fonksiyonuna tabi tutulur. Ardından parçalar çaprazlanarak bir sonraki çevrime gönderilir.



Şekil 3.3. Feistel yapı.

Şekil 3.4 teki gibi Genelleştirilmiş Feistel (GFN) yapısı Feistel yapısının daha gelişmiş halidir [3]. Çevrim girdisini birden çok alt bloğa bölüp fonksiyonu her parçaya uygular.



Şekil 3.4. Genelleştirilmiş feistel yapı.

Topla-Kaydır-XOR(ARX) yapısı şifreleme ve deşifreleme aşamasında S-box kullanımı yoktur. Burada yalnızca toplama, kaydırma ve XOR işlemleri vardır. Bu yapı oldukça hızlıdır ancak SPN ve Feistel' a kıyasla güvenlik özellikleri kısıtlıdır [41]. Doğrusal olmayan bir geri bildirim kaydırma Yazmacı (NLFSR) ise, giriş biti önceki durumunun doğrusal olmayan bir işlevi olan kaydırma yazmacıdır. Hibrit yapı, yukarıda bahsedilen beş yapıdan herhangi birkaçının birleştirilmesi ya da blok

şifreleme ile akış şifrelemenin birleştirilmesi ile elde edilir. Genel olarak Hafif Kriptografi' de bu yapılardan en çok SPN ve Feistel yapı kullanılmaktadır [3].

3.2.1.4. Hafif şifrelemede iç yapı

Hafif Kriptografi' de genel olarak hafızada kapladığı yerden kazanç sağlamak için AES' deki durumun aksine daha küçük blok boyları (128 bit yerine daha çok 64 bit ya da 80 bit) kullanılır. Genel olarak daha verimli olmak için şifrede küçük boyutlara sahip anahtarlar (96 bitten az) tercih edilir. Ancak NIST' e göre anahtar boyutu en az 112 bit olmalıdır. Hafif Kriptografi' de kullanılan işlemler ve bileşenler geleneksel kriptografiye göre daha basit yapıdadır. S-box olarak genelde 8 bit S-box yerine 4 bit S-box kullanılır. Böylece boyutları küçük kullanarak alandan büyük oranda tasarruf edilebilmektedir. Örneğin PRESENT şifresinde 4 bitlik S-box için 28 GE gerekirken AES' te 395 GE gerekir. Difüzyon katmanında ise karmaşık lineer katman yerine bit permütasyonu ya da tekrarlayan MDS matrisleri tercih edilir. Basit yapıda çevrim fonksiyonları kullanılması durumunda güvenliği sağlamak için çevrim sayısı daha fazla olmalıdır. Karmaşık anahtar üretim şemaları kullanıldığında gecikme, güç tüketimi ve hafızada kapladığı alan artar. Bu sebeple Hafif Kriptografi' de genel olarak daha basit anahtar üretim şemaları kullanılarak çevrim anahtarları üretilir. Bu durum bağlantılı, zayıf ya da seçilmiş anahtarlar kullanılarak yapılabilen bazı saldırılara sebebiyet verilebilir. Ancak bir anahtar üretim fonksiyonu kullanarak bu durumun önüne geçilebilir [42].

4. YENİ BİR ŞİFRE SİSTEMİ TASARIMI VE ÖLÇÜMÜ

Tezin bu bölümünde kaynak kısıtlı cihazlara uygulanabilen LALE isimli yepyeni bir Hafif Kriptografi algoritması tasarlandı. Yeni şifre tasarımı yapılmadan önce literatürdeki Hafif şifreleme sistemleri kapsamlı bir şekilde incelendi. İncelenen Hafif şifre sistemlerinin performans açısından karşılaştırmalarına bakıldığında şöyle sonuçlar elde edildi. Yazılım uygulaması açısından karşılaştırma yapıldığında Simon ve Speck algoritmalarının en iyisi olduğu gözlemlendi. Hafıza gereksinimi açısından karşılaştırıldığında Simon ve Speck algoritmaları 200 byte ROM ve 0 byte RAM ile sırasıyla en iyileridir. Donanım uygulaması açısından değerlendirildiğinde ise Midori ve Piccolo en iyileridir. Blok boyu ile anahtar boyunun donanıma etkisine bakıldığında ise SEA ve Hummingbird algoritmaları en iyi algoritmalardır. Kapladığı alan açısından kıyaslandığında ise KTANTAN algoritması 462 GE ile ilk sırada ve 503 GE ile Print şifresi ikinci sırada gelir. Enerji tüketimi açısından karşılaştırıldığında ise az farklarla sırasıyla Midori, Piccolo ve Prince şifreleri gelir. Dolayısıyla performans açısından yapılan karşılaştırmalar incelendiğinde, her alanda iyi olan bir şifre sisteminin mevcut olmadığı görülmektedir. Örneğin Simon şifresi yazılım uygulamasında ve hafıza gereksiniminde iyi iken enerji tüketimi konusunda iyi durumda değildir. Güvenlik ölçümleri açısından kıyaslandığında ise her şifrenin farklı bir saldırıya karşı dayanıksız olduğu görülmektedir. Yapılan incelemeler sonucunda sistemde kullanılan bileşenlerde yapılan farklı tasarım tercihlerinin, sistemleri bazı alanlarda avantajlı hale getirirken, bazı alanlarda dezavantajlı hale getirdiği gözlemlendi.

Bu incelemeler göz önünde bulundurularak her bileşeninin özenle tasarlandığı güvenli ve performanslı çalışan yepyeni bir şifreleme sistemi elde edildi. Şifrenin S-box katmanı, permütasyon katmanı, anahtar şeması, vb. bileşenleri ile yapısı hız-maliyet-güvenlik dengesi göz önüne alınarak tasarlanmıştır. Yeni sistemde, DNA tabanlı yepyeni bir yöntem geliştirilerek bu yöntem ile bir 4x4 S-box üretildi ve kullanıldı. Şifrede, analitik saldırılara karşı dayanıklılığı artırmak için anahtar beyazlatma aşaması kullanıldı. Çevrim sabiti ekleme aşaması hız ve maliyet dengesini sağlayacak

şekilde titizlikle geliştirildi. Sistemin iç yapısında SPN ve Feistel yapılarının bir arada kullanıldığı hibrit bir yapı tercih edildi. Şifrede SPN ve Feistel' ın kendine has özellikleri birleştirilerek ideal bir yapı elde edildi. Daha önce benzer bir çalışma yapılmadığı için yeni bir bakış açısı ile bu yapıların birarada kullanıldığı bir sistem tasarlandı. Elde edilen şifre sisteminin güvenlik ve performans analizleri yapıldı. Yaptığımız güvenlik analizleri sonucuna göre şifremiz diferansiyel kriptanaliz, integral saldırısı ve öz-benzerlik saldırısı gibi bilindik saldırı tekniklerine karşı dayanıklıdır. Diferansiyel aktif S-box sayıları oldukça yüksek olan yeni şifre sisteminin diğer şifre sistemleri ile olan karşılaştırmaları verildi. Elde edilen sonuçlara göre yeni şifre sistemi LALE, diğerlerine göre çok daha güvenlidir. Yapılan yazılım uygulaması ile yeni şifre sisteminin diğer algoritmalarla hız karşılaştırmalarına bakıldığında LALE'nin diğer algoritmalara göre çok daha hızlı olduğu gözlemlendi.

Bu bölümde yeni sistemin içeriğinde kullanılan bileşenlerin tasarım özellikleri ve tercih sebeplerinden bahsedilmiştir. Ardından yapılan güvenlik ve performans analizleri açıklanarak sonuçları paylaşılmıştır.

4.1. Yeni Şifre Sisteminin Yapısı

Yeni şifre sistemi, genel uygulamalara uygun olması açısından 64-bit blok boyu ve yeterli güvenlik seviyesini sağlayabilmek için 128-bit anahtar boyunu destekleyen bir şifre sistemidir. Yapı olarak SPN ve Feistel yapıyı birleştiren hibrit bir yapı tercih edilmiştir. Genel olarak literatürdeki hafif şifre sistemlerinde SPN ya da Feistel yapı tercih edildiği gözlemlenmiştir. Blok şifrelerin yapı çeşitlerinden olan SPN ve Feistel kolay uygulanabilirlik açısından en uygun olanlarıdır [3]. Ancak bu yapıların kendine has avantajları ve dezavantajları vardır. Feistel yapıda çevrim fonksiyonu yalnızca girdinin bir yarısına uyguladığı için bu yapıdaki bir şifre donanımda daha az güç tüketir. Feistel tipi yapılar, her çevrimde girdinin yalnızca yarısında doğrusal-olmama durumu ortaya koyar ve bu nedenle güvenliğin yeterli düzeyde olması için Feistel' daki çevrim sayısı SPN' e göre daha fazla olmalıdır [4]. Yani SPN, Feistel yapılara göre daha az çevrim sayısı ile yeterli güvenliği sağlayabilir. Bu nedenle SPN' in az çevrim sayısı kullanma özelliği ile Feistel' ın çevrim fonksiyonunu bloğun yarısına uygulama özelliğinin bir arada kullanıldığı Hibrit bir yapı tasarlanmıştır. Yeni şifre sisteminde çevrim sayısı 10-2 şeklindedir. Buna göre SPN kısımda çevrim sayısı 10 iken Feistel kısmında çevrim sayısı 2'dir. Tablo 4.4'te verilen diferansiyel aktif S-box

sayısı değerlerine göre, istenilen güvenlik seviyesi göz önünde bulundurularak 8-2, 12-2 ya da 16-2 çevrim sayıları da tercih edilebilir. Yeni şifre sisteminde, yeterli güvenlik seviyesini sağlamak ve daha az enerji harcamak için çevrim sayısı az olacak şekilde SPN ve Feistel yapı birleştirilmiştir. LALE' nin şifreleme ve deşifreleme fonksiyonları oldukça benzerdir. Dolayısıyla şifreleme ve deşifreleme fonksiyonları için gerekli olan fiziksel gereksinimler ve uygulama süreleri hemen hemen aynıdır.

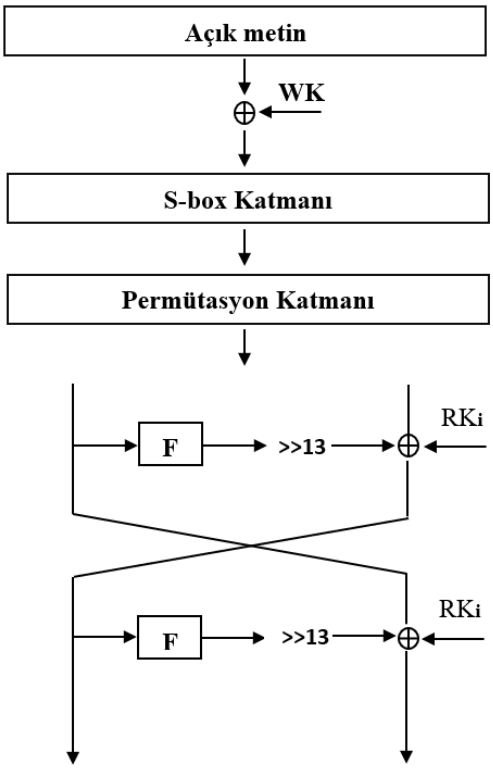
Bu bölümde yeni şifre sisteminin şifreleme algoritması ve içerdiği bileşenlerinin yapısından, tercih sebeplerinden ve diğer Hafif şifre sistemleri ile olan karşılaştırmalarından ayrıntılı olarak bahsedilmiştir. Ardından anahtar şeması ve deşifreleme algoritması verilmiştir. Bu bölümde kullanılacak olan simgeler ve kısaltmalar aşağıdaki gibidir.

Pl : 64-bit açık metin
WK : 64-bit Beyazlatma anahtarı (Whitening key)
S : 4x4 S-box
P : 64-bit Permütasyon
$A \| B$: A ve B bit dizilerinin ard arda bağlanması
F : Çevrim fonksiyonu
RC_i : i. çevrimde kullanılan 32-bit Çevrim sabiti
RK_i : i. çevrimde kullanılan 32-bit Çevrim anahtarı
K : 128-bit Ana anahtar
>>13: 13-bit Sağ çevrimsel kaydırma işlemi
C : 64-bit Şifreli metin
$\oplus$: Bit bazında özel-OR işlemi (XOR)

4.2. Şifreleme Algoritması

Şifreleme aşamasında girdi, 64-bitlik bloklara bölünür ve bloklar ayrı ayrı şifrelenir. Tasarlanan yeni şifre sistemi Şekil 4.1'de gösterildiği gibi iki aşamadan oluşmaktadır. İlk aşama SPN yapıdadır ve şu işlemlerden oluşur. İlk olarak tek sayılı çevrimlerde 64-bit girdi ile beyazlatma anahtarı XORlanır. Elde edilen çıktı 4-bitlik bloklara ayrılarak S-box işlemine tabi tutulur. S-box katmanından elde edilen 4-bitlik çıktılar tekrar birleştirilerek 64-bit blok elde edilir ve permütasyon işlemine tabi tutulur. İkinci aşama 2-çevrim yinelemeli Feistel yapısıdır. Başlangıçta SPN kısımdan elde edilen 64-bitlik çıktı iki eşit parçaya ayrılır. Buna göre, X1||X0 Feistel yapının sırasıyla 32-bit sol parça ve 32-bit sağ parça girdisi olarak alalım. İlk olarak X1 ile çevrim sabiti XORlanır ve ardından S-box işlemine tabi tutulur. Böylece F(X1) fonksiyonu hesaplanır. Akabinde elde edilen 32-bit çıktıya 13-bit sağ çevrimsel kaydırma işlemi

yapılır. Son olarak, elde edilen çıktı, X0 ve çevrim anahtarı ile XORlama işlemine tabi tutulur. Feistel yapıda bu işlem ardarda 2 kez yapılır.



Şekil 4.1. Yeni şifre sistemi LALE'nin şifreleme algoritması.

10 çevrim şifreleme algoritması aşağıdaki gibidir.

1. $V = Pl$
2. For $i = 1, 2, ..., 10$ do
3. if $i\%2 == 1$
4. $V = V \oplus WK$
5. $V = S(V)$
6. $V = P(V)$
7. $X_0 = [V_{31}\ V_{30} \ldots\ V_0]$
8. $X_1 = [V_{63}\ V_{62} \ldots\ V_{32}]$
9. For $j = 1, 2$ do
10. $X_{j+1} = (F(X_j) >> 13) \oplus RK_i \oplus X_{j-1}$
11. $V = X_2 \,||\, X_3$
12. $C = V$

4.2.1. Anahtar beyazlatma aşaması

Sistemi saldırılara karşı daha dirençli hale getirmek için tek sayılı çevrimlerde Anahtar beyazlatma işlemi kullanılmaktadır. DES' in anahtar boyu 56-bit olduğu için Kaba Kuvvet saldırılarına karşı dirençli bir sistem değildir. DES'i Kaba Kuvvet saldırısına karşı dirençli hale getirmek için DES'e anahtar beyazlatma aşaması eklenerek DESX şifreleme sistemi elde edilmiştir. DESX, FEAL, RC6, Twofish, vb. gibi şifre sistemlerinde anahtar beyazlatma işlemi kullanılmıştır. Tasarladığımız yeni şifre sisteminde kullanılan anahtar beyazlatma aşaması diğer şifre sistemlerinde kullanılan beyazlatma aşamalarından biraz farklıdır. Buna göre anahtar beyazlatma aşaması, saldırılara karşı direnci artırmak ve enerji tüketimini azaltmak için yalnızca tek sayılı çevrimlerde 64-bit girdi ile 128-bit ana anahtardan elde edilen beyazlatma anahtarı XORlanarak yapılır. S, 4x4 S-box ve K, ana anahtar olmak üzere WK anahtarı aşağıdaki şekilde elde edilir. İlk olarak 128-bit ana anahtarın son 64-biti 4-bitlik alt bloklara bölünüp tek tek S-box işlemine tabi tutulur. Ardından elde edilen çıktılar tekrar aynı sırada birleştirilerek 64-bitlik Beyazlatma anahtarı elde edilir.

$$K = [k_{127}\ k_{126} \ldots k_1\ k_0] \tag{4.1}$$

$$WK = S[k_{127}\ k_{126} \ldots k_{65}\ k_{64}] \tag{4.2}$$

4.2.2. S-box

S fonksiyonu, şifrenin lineer olmayan katmanını temsil eder. Şifrede kullanılan S fonksiyonu Tablo 4.1.' de de gösterildiği gibi 4 bitten 4 bite tanımlı bir S-box' tır.

Tablo 4.1. Yeni şifre sistemi LALE'nin S-box fonksiyonu.

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
S(x)	A	1	D	8	6	0	C	F	7	E	B	4	5	3	9	2

Karıştırma fonksiyonu olarak 4-bitlik veriyi karıştıran, güç tüketimini önemli ölçüde düşüren yalnız bir tane 4x4 S-box tablosu kullanılmaktadır. Basit yazılım ya da donanım uygulamaları açısından çoklu S-box tablosu kullanmak yerine tek bir S-box kullanmak daha uygundur [6]. Uygulama açısından donanımda en önemli husus alan gereksinimidir. Donanımda uygulama açısından 8x8 S-box yerine daha küçük olan 4x4 S-box kullanmanın avantajı daha çoktur [18]. Aynı zamanda 4x4 S-box kullanmak döngü başına harcanan enerji açısından 8x8 S-box' a göre daha etkilidir. Bunun sebebi

4x4 S-box' da 8x8 S-box' a göre daha düşük sinyal gecikmesi yaşanmasıdır. Bu bilgileri göz önünde bulundurarak yepyeni bir yaklaşımla DNA tabanlı 4x4 S-box tasarlama yöntemi geliştirilmiş ve kullanılmıştır. Kullanılan 4x4 S-box Diferansiyel/ Lineer aktif S-box sayısını hızlıca artırmaktadır. Ayrıca şifrede kullanılan S-box şu şartları sağlayacak şekilde oluşturulmuştur: Denge (Balanced), Bütünlük (Completeness), Çığ kriteri (Avalanche criterion), Bağımsız bit (Bit Independence), vb. [43]. Yeni geliştirilen 4x4 S-box tasarlama sistemi aşağıda ayrıntılı bir şekilde açıklanmıştır.

4.2.2.1. DNA tabanlı 4x4 S-box tasarımı için yeni bir yöntem

Şifrede, DNA tabanlı yepyeni bir yaklaşım kullanılarak 4x4 S-box elde edilmiştir. DNA tabanlı şifreleme yöntemine göre her ikili bit bir baz olarak kabul edilir. Örneğin bir byte 8 bitten oluştuğu için burada 4 tane baz bulunur. Örneğin, 01001110 bit dizisi, CATG DNA dizisi şeklinde ifade edilir. 4x4 S-box yapısı 4 bitlik elemanlardan oluşur. 4 bit uzunluğa sahip bir bit dizisinin alabileceği en fazla 16 farklı değer vardır ve bunlar $d_1d_2d_3d_4 \in \{0,1,...,15\}$ şeklindedir. Aşağıda yeni 4x4 S-box üretmek için izlenecek adımlar verilmiştir.

1) İlk olarak $\{0,1,...,15\}$ kümesindeki sayılar 4 farklı kümeye (a,b,c,d) ayrılır. Bunun için basit bir yerleştirme yöntemi kullanılır. Buna göre ilk olarak bir k başlangıç değeri seçilir. k,k_1,k_2,k_3 değişkenleri rastgele değerler olmak üzere, a kümesine alınacak elemanlar k , b kümesine alınacak elemanlar $k+k_1$, c kümesine alınacak elemanlar $k+k_2$ ve d kümesine alınacak elemanlar $k+k_3$ ile belirlenir. Böylece, ($k=0, k_1=1, k_2=2, k_3=3$ ve $n=4$ olmak üzere)

$$a=k, b=k+k_1, c=k+k_2, d=k+k_3 \; ; \forall k=\{0,1,...,16\}, k=k+n \qquad (4.3)$$

işlemleri sonucunda,

$$a=(0,4,8,12), b=(1,5,9,13), c=(2,6,10,14), d=(3,7,11,15) \qquad (4.4)$$

olarak elde edilir. Ardından sayıların karşılık geldiği bit dizisindeki ikililer, (00 = A, 01=C, 10=G, 11=T) kullanılarak A,C,G,T bazlarına dönüştürülür.

2) İlk bölümde elde edilen dört kümeye özel işlemler yapmak suretiyle tek bir kümeye indirgeme işlemi yapılır. DNA iplikçiğini tamamlamak için 3'-

ucundan 5'-ucuna ve 5'-ucundan 3'-ucuna olan iplikçikleri aşağıda verilen sırada birleştirelim:

İplikçik = Düz sırada(a) + Ters sırada(b) + Düz sırada(c) + Ters sırada(d)

Düz sırada() : Dizideki elemanlar olduğu sıra ile alınır.

Ters sırada() : Dizideki elemanlar ters sıra ile alınır.

3) Her bir dörtlü DNA dizisine sırasıyla Watson Crick Tamamlama yöntemi ve ters alma işlemi uygulanır. Watson Crick Tamamlama yöntemine göre A yerine T, T yerine A, C yerine G ve G yerine C yazılır.

D , 4 bitlik bir DNA dizisi ve $1 \le i \le 4$ için $d_i \in \{A, C, G, T\}$ olmak üzere $D = d_4 d_3 d_2 d_1$ olsun. D 'nin tamamlayıcısı $D^c = d_4' d_3' d_2' d_1'$ dir. A $\Leftrightarrow$ T ve C $\Leftrightarrow$ G için AGTC $\Leftrightarrow$ TCAG dir. D nin tersi $D^r = d_2 d_1 d_4 d_3$ şeklindedir. Diğer bir ifade ile $D^{rc} = d_2' d_1' d_4' d_3'$ dir. Örneğin $D =$ AGTC için $D^{rc} =$ AGTC dir.

4) Son olarak, DNA dizisinin rastgeleliğini iki katına çıkarmak için son aşamada elde edilen DNA dizisi ile herhangi bir rastgele DNA dizisi XOR işlemine tabi tutulur. Rastgele DNA dizisini birçok yöntemle elde etmek mümkündür. Mesela bu diziler GenBank sitesinden ya da herhangi bir rastgele sayı üreteci kullanarak elde edilebilir. R rastgele sayı üreteci olmak üzere,

$$D = D^{rc} \oplus \mathrm{R} \qquad (4.5)$$

DNA dizisi elde edilir.

5) Son olarak elde edilen bu DNA dizisinde (A=10, C=11, G=01, T=00) ile dekodlama işlemi yapılır. Elde edilen son dizi yeni 4x4 S-box'tır.

4.2.3. Yayılma fonksiyonu

Şifrenin lineer katmanı için donanımda herhangi bir maliyet gerektirmeden uygulanabilen bit bazlı permütasyon işlemi kullanılmıştır. Literatürdeki şifre sistemlerinde genel olarak bit bazlı permütasyon işlemi kullanılır. Ancak bazı sistemlerde kelime bazlı permütasyon işlemi kullanıldığı da görülmüştür. Sistemde kullanılan bit bazlı permütasyon işlemi Diferansiyel/ Lineer aktif S-box sayısını ve yayılımı hızla artıracak şekilde tercih edilmiştir. P Yayılma fonksiyonu Tablo 4.2 de gösterildiği gibi 64-bit girdinin i. bitinin $P(i)$ 'ye gittiği bir permütasyon işlemidir.

64-bit girdide her bir bit tablodaki gösterilen bit ile değiştirilir. Örneğin yeni 64-bit girdinin 0. bitine , mevcut 64-bit girdinin belirtilen 56. biti getirilir.

Tablo 4.2. Yayılma fonksiyonu.

İ	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
P(i)	56	47	38	29	20	11	2	64	55	46	37	28	19	10	1	63
i	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
P(i)	54	45	36	27	18	9	62	53	44	35	26	17	8	61	52	43
İ	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
P(i)	34	25	16	7	60	51	42	33	24	15	6	59	50	41	32	23
i	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
P(i)	14	5	58	49	40	31	22	13	4	57	48	39	30	21	12	3

4.2.4. Çevrim sabiti ekleme

Reflection, Slide ve Slidex gibi bazı saldırılar çevrim fonksiyonundaki benzerlikleri kullanır [14]. Çevrim fonksiyonları arasındaki benzerlikleri ortadan kaldırmak ve bu saldırılara karşı dayanıklı olmak için sistemde çevrim sabiti kullanılmıştır. Mikro denetleyicilerde sadece şifreleme aşamasının olması gibi bir durumda hafızada daha az yer kaplaması açısından çevrim sabitleri bir tablo ve fonksiyon kullanılarak hesaplanmaktadır. Kullandığımız yöntem, diğer şifre sistemlerinde kullanılan yöntemlerden farklı olan ITUbee' nin çevrim sabiti ekleme yönteminden esinlenerek oluşturulmuştur. Bu işlem 32-bit girdi ve çevrim sabitinin XORlanması ile gerçekleştirilir. Sistemde 16 adet 32-bit çevrim sabiti vardır. Feistel aşamasında iki çevrim sabiti kullanılır. 10 Çevrim için 10 adet Çevrim sabiti üretmek yeterlidir. 16 çevrim tercih edilmesi durumunda 16 adet çevrim sabiti üretilmelidir. Bu çevrim sabitleri aşağıda verilen fonksiyon ve 4.3. te verilen çevrim sabiti hesaplama tablosu ile elde edilir.

Tablo 4.3. Çevrim sabiti hesaplama tablosu.

0	1	2	3	4	5	6	7
0xAA	0xD8	0x55	0x0F	0xF0	0x3C	0x5C	0x18
8	9	10	11	12	13	14	15
0x66	0xB8	0x91	0x64	0x94	0xC9	0x2E	0xF8

$(j = 0,1,\ldots,15)$ için $f(j)=RC_{j+1} = (0x15 - j) \,||\, (0x14 - j) \,||\, (0x13 - j) \,||\, (0x12 - j)$

(4.6)

Örnek:

$$f(0)=RC_1 = (0x15)||(0x14)||(0x13)||(0x12)$$
$$= (0xF8)||(0x2E)||(0xC9)||(0x94)$$
$$= 0xF82EC994$$

4.2.5. Çevrim fonksiyonu

Yeni şifre sisteminde her bir Feistel çevrimi için ayrı bir çevrim fonksiyonu vardır. Bu fonksiyon Feistel aşamasındaki her çevrimde ayrı bir fonksiyon olacak şekilde kullanılır. Fonksiyonlardaki farklılıklar, her çevrimde farklı bir çevrim sabitinin eklenmesiyle elde edilir. Bu yöntemle sistemdeki karmaşıklık artırılır. RC_i ile çevrim sabiti ve S ile S-box' ı ifade eden çevrim fonksiyonu aşağıdaki gibidir. Buna göre 32-bit girdi ile $i.$ çevrim sabiti XORlanır. Elde edilen çıktıya 4x4 S-box işlemi uygulanır. Yapılan işlemler sonucunda ise yine 32-bit çıktı elde edilir.

$$F : \{0,1\}^{32} \rightarrow \{0,1\}^{32}$$
$$X, RC_i \rightarrow F(X, RC_i) = S(X \oplus RC_i)$$

4.3. Anahtar Şeması

Yeni şifre sistemi LALE'nin anahtar şeması, diğer birçok hafif blok şifre sistemine benzer olarak akış şifreleme yöntemi kullanılarak tasarlanmıştır. Present ve diğer bazı hafif şifre sistemleri Anahtar benzerlik saldırılarına karşı etkili olan bu yöntemi kullanmışlardır. Anahtar şeması çevrim anahtarları arasında benzerlik olmayacak şekilde titizlikle geliştirilmiştir. Çevrim anahtarlarını üretmek için basit kaydırma işlemi, doğrusal olmayan işlem ve XOR işlemi kullanılmıştır. İlk olarak donanımda maliyetsiz olarak uygulanabilen 48-bit üzerinde sola-kaydırma işlemi uygulanır.

Performans ve güvenlik açısından dengede olması için belirli bir 8-bit' lik parçaya 4x4 S-box uygulanır. Son olarak çevrim sabiti ile XOR işlemi yapılır.

128-bit ana anahtar K, bir $K = k_{127}k_{126}\ldots k_1k_0$ anahtar sayacına alınır. Mevcut K sayacının ise sağ 32-biti ilk çevrim anahtarı olan RK_1' dir. Diğer çevrim anahtarları için K sayacını güncelleme yöntemi aşağıdaki gibidir.

$i = 2,3,\ldots,16$ için,

1) $K <<< 48$
2) $[k_{25}k_{24}k_{23}k_{22}k_{21}k_{20}k_{19}k_{18}] \oplus RC_i$
3) $[k_{16}k_{15}k_{14}k_{13}] = S[k_{16}k_{15}k_{14}k_{13}]$

   $[k_{12}k_{11}k_{10}k_9] = S[k_{12}k_{11}k_{10}k_9]$
4) $K = [k_{127}k_{126}\ldots k_1k_0]$

İlk olarak K sayacı 48-bit sola kaydırılır. Ardından K' nın $k_{25}k_{24}k_{23}k_{22}k_{21}k_{20}k_{19}k_{18}$ biti ile i. çevrim sabitinin sağdan ilk 8-biti XOR işlemine tabi tutulur ve $k_{16}k_{15}k_{14}k_{13}k_{12}k_{11}k_{10}k_9$ bitleri doğrudan S-box' a alınır. Son olarak elde edilen K sayacının sağ 32-bitini i. çevrim anahtarı RK_i olarak elde edilir. Her bir çevrim anahtarını üretirken yukarıdaki işlemler tekrarlanır. 10 çevrim şifreleme için 10 tane, 16 çevrim için 16 tane çevrim anahtarı üretilir.

4.4. Deşifreleme Algoritması

Yeni şifre sistemi LALE'nin şifreleme ve deşifreleme aşaması hemen hemen aynıdır. Aralarındaki tek fark deşifreleme kısmında S-box işlemi ile permütasyon işleminin tersi kullanılır. Bu nedenle şifreleme ve deşifreleme aşamasındaki fiziksel maliyet yaklaşık olarak aynıdır. Feistel kısmının deşifreleme işleminde girdi, şifrelenmiş metindir ve çevrim anahtarları sistemde ters sırada kullanılır. SPN kısmın deşifrelenmesinde ise yalnızca S-box ve permütasyon işlemlerinin tersi kullanılır. Deşifreleme algoritmasında $X_i \,||\, X_{i+1}$ sırasıyla sol 32-bit girdi ile sağ 32-bit girdi ve S^{-1} S-box'ın tersini, P^{-1} ise P yayılım fonksiyonunun tersi olmak üzere aşağıdaki gibidir.

1. $V = C$
2. For $i = 10,9,\ldots,1$ do
3. $X_2 \| X_3 = V$
4. For $j = 1,0$ do
5. $X_j = \left(F\left(X_{j+1}\right) >> 13\right) \oplus X_{j+2} \oplus RK_i$
6. $V = X_1 \| X_0$
7. $V = P^{-1}(V)$
8. $V = S^{-1}(V)$
9. $if\ \ i\%2 == 1$
10. $V = V \oplus WK$
11. $Pl = V$

4.5. Güvenlik Ölçümü

4.5.1. Diferansiyel kriptanaliz

Diferansiyel Kriptanaliz en güçlü atak çeşitlerinden biridir [37]. Bir şifrenin bu saldırıya karşı dayanıklılığını değerlendirmek için Diferansiyel aktif S-box sayısını kullanırız. Şifrenin Diferansiyel aktif S-box sayısı Tablo 4.4' de gösterildiği gibidir.

Tablo 4.4. Diferansiyel aktif S-box sayısı.

Çevrim	1	2	3	4	5	6	7
Aktif S-box sayısı	1	2	7	20	35	50	66

Bu tabloya göre 5. çevrimde aktif S-box sayısı en az 35 olarak ölçülmüştür. 10 çevrim için aktif S-box sayısını hesaplayacak olursak en az $35 \times 2 = 70$ aktif S-box olarak elde ederiz. Dolayısıyla, diferansiyel olasılığı,

$$\varepsilon = 2^{(aktif\ S-box\ sayısı-1)} \times (Max.Bias)^{(aktif\ S-box\ sayısı)} \quad (4.7)$$

$$= 2^{(70-1)} \times 2^{-105} = 2^{-36} \quad (4.8)$$

şeklindedir. Bilinen-açık metinler için karmaşıklık $C = 1$ olması durumunda

$$N_L = 1/(\varepsilon)^2 \quad (4.9)$$

ile hesaplanır. Buna göre 10 çevrim için gereken toplam seçilen-açık metin sayısı 2^{72} ’dır ki bu 2^{64} ’ ten oldukça büyüktür. Dolayısıyla 64-bit blok boyu kullanan yeni şifre sistemi, Diferansiyel Kriptanaliz’ e karşı dayanıklıdır. Tablo 4. 5’te yeni şifre sistemi LALE’nin diferansiyel dağılım tablosu verilmiştir.

Tablo 4.5. Yeni şifre sistemi LALE’nin diferansiyel dağılım tablosu.

		Output Difference															
		0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
I	0	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
n	1	0	0	0	2	0	2	4	0	0	2	0	4	0	0	0	2
p	2	0	2	0	0	0	0	0	2	0	2	4	0	4	0	0	2
u	3	0	0	2	2	0	2	0	2	0	2	2	0	4	0	0	0
t	4	0	4	4	0	0	0	2	2	0	0	0	0	2	2	0	0
	5	0	0	2	0	4	0	0	2	0	2	2	2	0	2	0	0
D	6	0	0	0	0	0	0	2	2	2	0	0	2	2	0	6	0
i	7	0	2	0	0	0	4	0	2	2	0	0	0	0	4	2	0
f	8	0	0	0	4	0	2	2	0	0	0	0	0	2	4	0	2
f	9	0	0	0	2	2	4	4	0	0	2	0	0	0	0	2	0
e	A	0	2	2	0	0	2	2	0	0	2	2	0	2	0	0	2
r	B	0	0	0	2	2	0	0	0	0	2	4	0	0	0	2	4
e	C	0	2	2	0	2	0	0	2	0	0	2	2	0	0	2	2
n	D	0	2	0	0	4	0	0	2	4	2	0	0	0	0	0	2
c	E	0	2	0	4	2	0	0	0	2	0	0	4	0	2	0	0
e	F	0	0	4	0	0	0	0	0	6	0	0	2	0	2	2	0

Aşağıda Tablo 4.6 da yeni şifre sisteminin ve diğer şifre sistemlerinin blok uzunluğu, anahtar boyu, S-box boyutu, çevrim sayısı ve iç yapısı bilgileri verilmiştir. Bu şifre sistemlerinin diferansiyel aktif S-box sayıları yönünden yeni tasarlanılan şifre sistemi LALE ile olan karşılaştırma tablosu Tablo 4.7 de verilmiştir.

Tablo 4.6. Yeni şifre sistemi LALE’nin bazı yönlerden karşılaştırması.

Şifreleme sistemleri	AES	Klein	LED	LBlock	Twine	Midori	Present	LALE
Blok	128	64	64	64	64	64/128	64	64
Anahtar	128/192/256	64/80/96	64/128	80	80/128	128	80/128	128
S-box boyutu	8x8	4x4	4x4	4x4	4x4	4x4	4x4	4x4
Çevrim	10/12/14	12/16/20	8/12	32	36	16/20	31	10/2
İç yapısı	SPN	SPN	SPN	Feistel	GFS	SPN	SPN	Hibrit

Tablo 4.7. Yeni şifre sisteminin (LALE) diğer şifre sistemleri ile diferansiyel aktif S-box sayıları açısından karşılaştırması.

Çevrim sayısı / Şifreleme sistemleri	AES (8x8)	Klein (4x4)	LED (4x4)	LBlock (4x4)	Twine (4x4)	Midori (4x4)	Present (4x4)	LALE (4x4)
1.çevrim	1	1	-	0	0	-	-	1
2.çevrim	5	5	-	1	1	-	-	2
3.çevrim	9	8	-	2	2	-	-	7
4.çevrim	25	15	25	3	3	16	8	20
5.çevrim	26	16	-	4	4	23	10	35
6.çevrim	30	20	-	6	6	30	12	50
7.çevrim	34	23	-	8	8	35	14	66

Buna göre yeni şifre sisteminin 7. çevrimde sahip olduğu aktif S-box sayısı 66 iken AES'te 34, Klein'de 23, Lblock ve Twine'da 8, Midori'de 35 ve Present'te 14 olarak ölçülmüştür. Dolayısıyla yapılan diferansiyel atağa göre elde edilen veriler neticesinde, yeni şifre sisteminin birçok şifre sistemine kıyasla daha yüksek diferansiyel aktif S-box sayısına sahip olduğu gözlemlenmiştir. Dolayısıyla yeni şifre sisteminin diğer şifre sistemlerine göre daha güvenli olduğu görülmektedir.

4.5.2. İntegral saldırısı

İntegral saldırısı yapısal saldırıların bir çeşididir [44]. Bu saldırılar AES tipindeki şifreler için uygundur. AES ve benzeri şifreler güçlü byte temelli şifrelerdir. Yeni şifre sistemi bit temelli bir şifre çeşididir ve aynı zamanda yayılma katmanında kullanılan permütasyon işlemi de bit temellidir. Dolayısıyla şifrede kullanılan bit bazında işlemler byte bazında birleşme ve yayılımı engellemektedir. Dolayısıyla yeni şifre sistemi İntegral saldırısına karşı dirençlidir.

4.5.3. Kendine-Benzerlik saldırısı

Reflection, Slide ve Slidex gibi Kendine-Benzerlik saldırıları çevrim fonksiyonları arasındaki benzerlikleri kullanmak suretiyle yapılan saldırılardır [45-47]. Bu şifrede

her çevrim için başka 32-bit çevrim sabiti vardır ve bu sabitler girdi ile XOR' lanır. Böylece çevrim fonksiyonları arasında yeterli miktarda farklılık elde edilir. Ayrıca anahtar şemasında her çevrim anahtarını üretirken farklı bir çevrim sabiti kullanılmaktadır. Dolayısıyla biz inanıyoruz ki, şifrede kullanılan anahtar üretme ve çevrim sabiti ekleme işlemi çevrim fonksiyonları arasındaki benzerliği ortadan kaldırır ve Reflection, Slide ve Slidex saldırılarına karşı dayanıklılığı sağlar.

4.6. Performans Ölçümü

Bu bölümde geliştirilen hafif sıklet şifreleme algoritması LALE'nin yazılım uygulama ve test işlemleri yapılarak hız ve Ram ölçümleri verilmiştir. Test işlemleri Intel(R) Core(TM) i7-8565U CPU @ 1.80GHz 1.99 GHz 8,00 GB 64 bit işletim sistemi, x64 tabanlı işlemciye sahip bir bilgisayarda, Ubuntu 20.04 64-bit işletim sistemi üzerinde gerçekleştirilmiştir. Program C++ programlama dilinde kodlanmıştır. Algoritma tasarımı farklı çevrim sayıları ve girdi dosya boyutları için test edilmiş, şifreleme ve deşifreleme süreleri tespit edilmiştir. Tablo 4.8'de çevrim sayıları 8,10,12 ve 16 ve giriş dosya boyutu olarak 8 byte 100 Kb. arasında farklı değerler için şifreleme ve çözme sürelerine ait değerler görülmektedir.

Tablo 4.8. Farklı dosya boyutları ve çevrim sayıları için şifreleme ve deşifreleme süreleri (mikrosaniye).

Girdi Boyutu/ Çevrim Sayısı		8.çevrim	10.çevrim	12.çevrim	16.çevrim
8 byte	Şifreleme	59	72	86	118
	Deşifreleme	58	74	85	113
32 byte	Şifreleme	218	269	321	427
	Deşifreleme	224	280	379	459
128 byte	Şifreleme	889	1106	1306	1717
	Deşifreleme	938	1234	1367	1807
512 byte	Şifreleme	3636	4606	5693	7069
	Deşifreleme	3685	4742	5770	7619
1 Kbyte	Şifreleme	7247	9807	10854	14923
	Deşifreleme	7669	9464	11507	15407
10 Kbyte	Şifreleme	89814	110241	135950	173945
	Deşifreleme	95621	113706	128978	178440
100 Kbyte	Şifreleme	853385	1033000	1276000	1589000
	Deşifreleme	916265	1088000	1306000	1664000

Yapılan kriptanaliz çalışmalarında algoritmanın 10 çevrim için ataklara dayanıklı olduğu gösterilmiştir. Bu sebeple geliştirilen algoritma için temel çevrim sayısı 10 olarak belirlenmiştir. Fakat ihtiyaç duyulması halinde farklı uygulamalar için çevrim sayısı güvenlik analiz sonuçları dikkate alınarak artırılıp azaltılabilir. Ayrıca her bir çevrim ve dosya girdi boyutu değerleri için şifreleme ve deşifreleme sürelerinin

birbirine yakın olduğu görülmektedir. Test sonuçlarına göre, algoritma 1KB veriyi 10 çevrim için ortalama 0.009 sn'de şifrelerken, 16 çevrim için bu değerin çok küçük bir artışla 0,014 sn'ye çıktığı tespit edilmiştir.

Tablo 4.9 da 10 çevrim LALE ile diğer algoritmaların şifreleme süreleri açısından saniye cinsinden karşılaştırma tablosu verilmiştir. Tablodaki sonuçlar 512 Byte girdi boyutuna sahip bir verinin şifrelenmesi için gereken süreleri gösterir. Buna göre yeni şifre sistemi AES, Lblock, Piccolo ve Present şifre sistemlerine göre çok daha hızlıdır.

Tablo 4.9. Şifreleme sistemlerinin 10 çevrimde hız yönünden karşılaştırması (sn).

Şifre sistemleri	AES	Lblock	Piccolo	Present	LALE
Şifreleme süreleri	≈ 0,012	≈0,012	≈0,09	≈0,9	≈0,0046

Aynı zamanda LALE'nin RAM ölçümleri de yapılarak Tablo 4.10 da verilmiştir. Buna göre 512 Byte büyüklüğündeki bir veriyi şifrelemek için gereken bellek miktarı 10 çevrim için 4,9 MB olarak ölçülmüştür. Sanal Bellek, işlemle eşlenen tüm kitaplıkları ve yürütülebilir nesneleri ve yığın alanını hesaplar. Yerleşik bellek ise, gerçekte RAM'de bulunan bellek miktarıdır.

Tablo 4.10. Yeni şifre sistemi LALE'nin RAM ölçümleri.

Girdi Boyutu/ Çevrim Sayısı		8.çevrim	10.çevrim	12.çevrim	16.çevrim
8 byte	Sanal Bellek	6,2 MB	6,2 MB	6,2 MB	6,2 MB
	Yerleşik Bellek	2,1 MB	2,1 MB	2,1 MB	2,1 MB
	Bellek	154,3 KB	162,3 KB	176,1 KB	180,2 KB
32 byte	Sanal Bellek	6,4 MB	6,4 MB	6,4 MB	6,4 MB
	Yerleşik Bellek	2,1 MB	2,1 MB	3,9 MB	3,8 MB
	Bellek	176,1 KB	180,8 KB	315,4 KB	323 KB
128 byte	Sanal Bellek	6,5 MB	6,5 MB	6,6 MB	6,8 MB
	Yerleşik Bellek	3,8 MB	3,8 MB	4,2 MB	4 MB
	Bellek	303,6 KB	319,5 KB	585,7 KB	589 KB
512 byte	Sanal Bellek	7,2 MB	7,4 MB	7,7 MB	8,1 MB
	Yerleşik Bellek	4,6 MB	4,9 MB	5,2 MB	5,4 MB
	Bellek	1,1 MB	1,4 MB	1,7 MB	1,9 MB
1 Kbyte	Sanal Bellek	8,2 MB	8,7 MB	9,2 MB	10,1 MB
	Yerleşik Bellek	5,4 MB	5,9 MB	6,5 MB	7,3 MB
	Bellek	1,9 MB	2,5 MB	3 MB	3,8 MB
10 Kbyte	Sanal Bellek	25,6 MB	30,3 MB	35 MB	44,6 MB
	Yerleşik Bellek	23 MB	27,6 MB	32,4 MB	41,9 MB
	Bellek	19,5 MB	24,1 MB	29 MB	38,4 MB
100 Kbyte	Sanal Bellek	199,2 MB	246,8 MB	294,3 MB	389,3 MB
	Yerleşik Bellek	196,5 MB	244,1 MB	291,4 MB	386,6 MB
	Bellek	193,1 MB	240,7 MB	288 MB	383,1 MB

5. SONUÇ VE ÖNERİLER

Bu çalışmada, ilk bölümde kriptolojinin önemi, IOT cihazlarında uygulanabilirliği ve hafif kriptografinin IOT cihazlarındaki yeri hakkında bilgilendirme yapıldı. İkinci bölümde bazı cebirsel tanımlar verilerek kriptoloji hakkında genel bilgilendirmeler yapıldı. Üçüncü bölümde ise hafif kriptografik bir sistem tasarlanırken dikkat edilmesi gereken hususlar hakkında yapılan literatür taramasından bahsedildi. Son bölümde yeni bir Hafif-siklet blok şifre sisteminin tasarımından ayrıntılı olarak bahsedildi. Yepyeni bir DNA tabanlı 4x4 S-box tasarım yöntemi geliştirildi. Bu yöntemin detayları tezde verildi. Yeni şifre sisteminin güvenlik ölçümleri ve performans analizleri yapıldı. Yapılan güvenlik ölçümlerine göre yeni şifre sistemi olası ataklara karşı diğer bazı algoritmalara göre daha yüksek güvenlik seviyesini sağladığı ispatlandı. Aynı zamanda yeni şifre sisteminin yazılım uygulaması yapıldı. Buna göre yeni sisteminin farklı dosya boyutları için şifreleme ve deşifreleme süreleri verildi. Yeni şifre sistemi LALE'nin diğer şifre sistemleri ile süre açısından karşılaştırmasına bakıldığında yeni sistemin diğer algoritmalara göre daha hızlı olduğu gözlemlendi. Sistemin farklı dosya boyutları ve çevrim sayıları açısından RAM ölçümleri yapıldı. İleride yeni şifre sisteminde başka tasarım tercihleri yapılarak daha etkili sonuçlar elde edilebilir. Donanımsal özellikleri açısından incelenerek diğer algoritmalarla karşılaştırmaları yapılabilir. Aynı zamanda çok etkili bir saldırı çeşidi olan Lineer atak yapılarak LALE'nin güvenliği başka yönden ispatlanabilir.

KAYNAKLAR

[1] M.H. Topaloğlu, N. Türk, B. (2016). Bilgi Güvenliği Kapsamında Yeni Bir Veri Şifreleme Algoritması Tasarımı ve Gerçekleştirilmesi. *Bilişim Teknolojileri Dergisi*, Cilt(9). https://dergipark.org.tr/tr/download/article-file/225394

[2] Patil, J., Bansod, G., & Kant, K. S. (2017, February). LiCi: A new ultra-Lightweight block cipher. In *2017 International Conference on Emerging Trends & Innovation in ICT (ICEI)* (pp. 40-45). IEEE., https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7977007

[3] Thakor, V. A., Razzaque, M. A., & Khandaker, M.R. (2021). Lightweight cryptography algorithms for resource-constrained IoT devices: A review, comparison and research opportunities. *IEEE Access, 9,* 28177-28193. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9328432

[4] Banik, S., Bogdanov, A., Isobe, T., Shibutani, K., Hiwatari, H., Akishita, T., & Regazzoni, F. (2016). Midori: A Block Cipher for Low Energy. *IEICE Technical Report; IEICE Tech. Rep.*, *116*(35), 45-45.

[5] Bogdanov, A., Knudsen, L. R., Leander, G., Paar, C., Poschmann, A., Robshaw, M. J., ... & Vikkelsoe, C. (2007). PRESENT: An ultra- lightweight block cipher. *In Cryptographic Hardware and Embedded Systems-CHES 2007: 9th International Workshop, Vienna, Austria, September 10-13, 2007.Proceeding 9* (pp. 450-466). Springer Berlin Heidelberg.

[6] Suzaki, T., Minematsu, K., Morioka, S., & Kobayashi, E. (2011, November). Twine: A lightweight, versatile block cipher. In *ECRYPT workshop on lightweight cryptography* (Vol. 2011). https://www.nec.com/en/global/rd/tg/code/symenc/pdf/twine_LC11.pdf

[7] Borgho, J., Canteaut, A., Guneysu, T., Kavun, E. B., Knezevic, M., Knudsen, L. R., ... & Yalcin, T. (2012). Prince-a low-latency block cipher for pervasive computing applications-proc. of advances in cryptology.

[8] Shibutani, K., Isobe, T., Hiwatari, H., Mitsuda, A., Akishita, T., & Shirai, T. (2011, September). Piccolo: An Ultra-Lightweight Blockcipher. In *CHES* (Vol. 6917, pp. 342-357). https://link.springer.com/content/pdf/10.1007/978-3-642-23951- 9.pdf#page=355

[9] Dobraunig, C. Eichlseder, M. Mendel, F. Schläffer, M. (2014). ASCON V1 Submission to the CEASAR Competition. Graz, Austria. https://competitions.cr.yp.to/round1/asconv1.pdf

[10] Akishita, T. Iwata, T. Moriai, S. Shibutani, K. Shirai, T. (2007). The 128-bit blockcipher CLEFIA (extended abstract). *Fast Software Encryption (FSE) (Lecture Notes in Computer Science)*, (vol. 4593). Springer.

[11] Kumar, M., Sk, P. A. L., & Panigrahi, A. (2014). FeW: a lightweight block cipher. *Turkish Journal of Mathematics and Computer Science, 11*(2), 58-73. https://dergipark.org.tr/en/download/article-file/914382

[12] Bansod, G., Patil, A., & Pisharoty, N. (2018). GRANULE: an ultra lightweight cipher design for embedded security. *Cryptology ePrint Archive.* https://eprint.iacr.org/2018/600.pdf

[13] Engels, D., Fan, X., Gong, G., Hu, H., & Smith, E. M. (2010). Hummingbird: ultra-lightweight cryptography for resource-constrained devices. In *Financial Cryptography and Data Security: FC 2010 Workshops, RLCPS, WECSR, and WLC 2010, Tenerife, Canary Islands, Spain, January 25-28, 2010, Revised Selected Papers 14* (pp. 3-18). Springer Berlin Heidelberg. https://link.springer.com/chapter/10.1007/978-3-642-14992-4_2

[14] Karakoç, F., Demirci, H., & Harmancı, A. E. (2013). ITUbee: a software oriented lightweight block cipher. In *Lightweight Cryptography for Security and Privacy: Second International Workshop, LightSec 2013, Gebze, Turkey, May 6-7, 2013, Revised Selected Papers 2* (pp. 16-27). Springer Berlin Heidelberg. https://link.springer.com/chapter/10.1007/978-3-642-40392-7_2

[15] Lai, X., & Massey, J. L. (1991). A proposal for a new block encryption standard. In *Advances in Cryptology—EUROCRYPT'90: Workshop on the Theory and Application of Cryptographic Techniques Aarhus, Denmark, May 21–24, 1990 Proceedings 9* (pp. 389-404). Springer Berlin Heidelberg. https://link.springer.com/chapter/10.1007/3-540-46877-3_35

[16] De Canniere, C., Dunkelman, O., & Knežević, M. (2009). KATAN and KTANTAN—a family of small and efficient hardware-oriented block ciphers. In *Cryptographic Hardware and Embedded Systems-CHES 2009: 11th International Workshop Lausanne, Switzerland, September 6-9, 2009 Proceedings* (pp. 272-288). Springer Berlin Heidelberg. https://link.springer.com/chapter/10.1007/978-3-642-04138-9_20

[17] Gong, Z., Nikova, S., & Law, Y. W. (2012). KLEIN: a new family of lightweight block ciphers. In *RFID. Security and Privacy: 7th International Workshop, RFIDSec 2011, Amherst, USA, June 26-28, 2011, Revised Selected Papers 7* (pp. 1-18). Springer Berlin Heidelberg. https://link.springer.com/chapter/10.1007/978-3-642-25286-0_1

[18] Wu, W., & Zhang, L. (2011). LBlock: a lightweight block cipher. In *Applied Cryptography and Network Security: 9th International Conference, ACNS 2011, Nerja, Spain, June 7-10, 2011. Proceedings 9* (pp. 327-344). Springer Berlin Heidelberg. https://link.springer.com/chapter/10.1007/978-3-642-21554-4_19

[19] Daemen, J., Peeters, M., Van Assche, G., & Rijmen, V. (2000, October). Nessie proposal: NOEKEON. *In First open NESSIE workshop* (pp. 213-230). https://perso.uclouvain.be/fstandae/source_codes/lightweight_ciphers/specs/NOEKEON.pdf

[20] Knudsen, L., Leander, G., Poschmann, A., & Robshaw, M. J. (2010). PRINTcipher: a block cipher for IC-printing. In *Cryptographic Hardware and Embedded Systems, CHES 2010: 12th International Workshop, Santa Barbara, USA, August 17-20, 2010. Proceedings 12* (pp. 16-32). Springer Berlin Heidelberg. https://link.springer.com/chapter/10.1007/978-3-642- 15031-9_2

[21] Zhang, W., Bao, Z., Lin, D., Rijmen, V., Yang, B., & Verbauwhede, I. (2014). RECTANGLE: a bit-slice lightweight block cipher suitable for Multiple platforms. *Cryptology ePrint Archive.* https://eprint.iacr.org/2014/084

[22] Beaulieu, R., Shors, D., Smith, J., Treatman-Clark, S., Weeks, B., & Wingers, L. (2013). The SIMON and SPECK families of lightweight block ciphers. *Cryptology eprint archive*. https://eprint.iacr.org/2013/404

[23] Beaulieu, R., Shors, D., Smith, J., Treatman-Clark, S., Weeks, B., & Wingers, L. (2013). The SIMON and SPECK families of lightweight block ciphers. *Cryptology eprint archive.* https://eprint.iacr.org/2013/404

[24] Andrews, B., Chapman, S., & Dearstyne, S. (2020). Tiny encryption algorithm (TEA) cryptography 4005.705. 01 graduate team ACD final report. *Rochester Inst. Technol., Rochester, NY, USA, Tech. Rep, 33695183.*

[25] Çallıalp, F. (2013). Örneklerle soyut cebir. Birsen Yayınları.

[26] Hungerford, T. W. (2012). Algebra (Vol. 73). Springer Verlag.

[27] Fraleigh, J. B. (2013). Soyut cebire giriş. (T. Öner, M. Terziler, Çev.) Palme Yayıncılık.

[28] Wan, Z. X. (2003). Lectures on finite fields and galois rings. World Scientific Publishing Co.

[29] Aydoğdu, S. (2017). Bazı özel matrislerden MDS matrislerin inşası [Yüksek lisans tezi]. Sakarya Üniversitesi.

[30] Vikipedi (2023). Kriptoloji. https://tr.wikipedia.org/wiki/Kriptoloji adresinden 22 Mart 2023 tarihinde alınmıştır.

[31] Merriam Webster (2022). Kriptoloji. https://www.merriam-webster.com/dictionary/cryptology adresinden 13 Ocak 2023 tarihinde alınmıştır.

[32] Paar, Christof. Pelzl, Jan. (2009). *Understanding Cryptography*. Springer, Germany.

[33] Stinson, D. R. (2002). *Cryptography Theory and Practice*. Chapman & Hall/CRC, USA.

[34] Swenson, C. (2008). *Modern Cryptanalysis.* Wiley Publishing, Inc., Canada.

[35] Smart, N. P. (2016). *Cryptography Made Simple.* Springer, UK.

[36] Wikipedia (2023). Cryptographic Protocol. https://en.wikipedia.org/wiki/Cryptographic_protocol adresinden 28 Mart 2023 tarihinde alınmıştır.

[37] Heys, H. M. (2002). A tutorial on linear and differential cryptanalysis. *Cryptologia*, 26(3), 189-221. https://ioactive.com/wp-content/uploads/2015/07/ldc_tutorial.pdf

[38] Talo, F. (2021). *DNA Tabanlı Kriptoloji Uygulaması* [Yüksek lisans tezi]. Düzce Üniversitesi.

[39] Gürsoy, F. (2019). *Değişmeli Olmayan Aykırı Polinom Halkaları üzerinde tanımlı DNA Kodlar* [Doktora Tezi]. Yıldız Teknik Üniversitesi.

[40] Panahi, P., Bayılmış, C., Çavuşoğlu, U., & Kaçar, S. (2021). Performance evaluation of lightweight encryption algorithms for IoT-based applications. *Arabian Journal for Science and Engineering*, 46, 4015-4037. https://link.springer.com/article/10.1007/s13369-021-05358-4

[41] Wikipedia (2023). Nonlinear-Feedback Shift Register. https://en.wikipedia.org/wiki/Nonlinear-feedback_shift_register adresinden 22 Mart 2023 tarihinde alınmıştır.

[42] McKay, K., Bassham, L., Turan, M. S., & Mouha, N. (2017). Report on lightweight cryptography (nistir8114). *National Institute of Standards and Technology(NIST)*.https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8114.pf

[43] Al-Wattar, A. S., Mahmod, R., Zukarnain, Z. A., & Udzir, N. I. (2015). Generating a new S-Box inspired by biological DNA. *International Journal of Computer Science and Application*, 4(1), 32-42. https://www.researchgate.net/publication/281507513_Generating_a_new_S-Box_inspired_by_biological_DNA

[44] Knudsen, L., & Wagner, D. (2002). Integral cryptanalysis. In *Fast Software Encryption: 9th International Workshop, FSE 2002 Leuven, Belgium, February 4–6, 2002 Revised Papers 9* (pp. 112-127). Springer Berlin Heidelberg. https://link.springer.com/chapter/10.1007/3-540-45661-9_9

[45] Kara, O. (2008, December). Reflection Cryptanalysis of Some Ciphers. In *INDOCRYPT* (Vol. 5365, pp. 294-307). https://link.springer.com/content/pdf/10.1007/978-3-540-89754-5.pdf#page=306

[46] Biryukov, A., & Wagner, D. (1999). Slide attacks. In *Fast Software Encryption: 6th International Workshop, FSE'99 Rome, Italy, March 24–26, 1999 Proceedings 6* (pp. 245-259). Springer Berlin Heidelberg. https://link.springer.com/chapter/10.1007/3-540-48519-8_18

[47] Dunkelman, O., Keller, N., & Shamir, A. (2012). Minimalism in cryptography: The Even-Mansour scheme revisited. In Advances in *Cryptology–EUROCRYPT 2012: 31st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cambridge, UK, April 15-19, 2012. Proceedings 31* (pp. 336-354). Springer Berlin Heidelberg. https://link.springer.com/chapter/10.1007/978-3-642-29011-4_21

ÖZGEÇMİŞ

Ad-Soyad : Fatma Betül PAK

ÖĞRENİM DURUMU:

- **Lisans** **:** 2020, Sakarya Üniversitesi, Fen-Edebiyat Fakültesi, Matematik Bölümü
- **Yükseklisans** **:** Devam ediyor, Sakarya Üniversitesi, Matematik Anabilim Dalı, Cebir ve Sayılar Teorisi Bilim Dalı

MESLEKİ DENEYİM VE ÖDÜLLER:

- 2020 yılında Sakarya Üniversitesi Dönemsel Başarı Ödülü'nü kazandı.

TEZDEN TÜRETİLEN ESERLER:

- Özen, M., Pak, F.B. ve Çavuşoğlu, Ü. 2023. LALE: A new Lightweight Blockcipher for IOT Platforms.