



**T.C.
SAKARYA ÜNİVERSİTESİ
BİLGİSAYAR VE BİLİŞİM BİLİMLERİ FAKÜLTESİ
BSM465-KRİPTOLOJİYE GİRİŞ**

ŞİFRELEME ALGORİTMASI TASARIMI

G201210382-Mehmet ATAŞ

Ders Grubu : 2. Öğretim A Grubu
Öğretim Görevlisi : Doç. Dr. Ünal ÇAVUŞOĞLU

Github

<https://github.com/mehatas/bsm465-kriptolojiyegiris>

Google Colab

https://colab.research.google.com/drive/1nzT_eSyVjj1c70iCo_g0VMNb9qHB5SSW?usp=sharing

2023-2024 Güz Dönemi

Literatür Taraması:

Simetrik Şifreleme

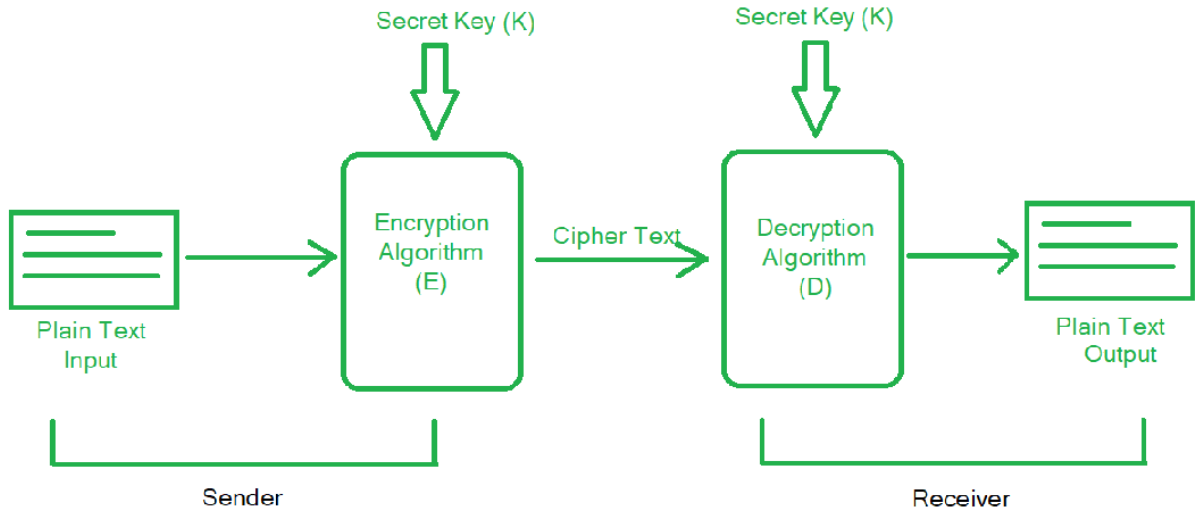
Simetrik Şifreleme, şifrelemenin en temel ve eski yöntemidir. Verilerin hem şifrelenmesi hem de şifresinin çözülme işlemi için yalnızca gizli bir anahtar kullanır. Bu nedenle Tek Anahtarlı Şifreleme olarak da bilinir.

Düz Metin: Gönderici ve alıcı arasında iletilecek orijinal mesaj.

Şifreli Metin: Orijinal mesajın insanlar tarafından anlaşılamayan şifrelenmiş hali.

Şifreleme: Düz metnin şifreli metne dönüştürülme işlemleri.

Şifre Çözme: Şifreli metnin orijinal düz metne dönüştürülmesi işlemleri.



Güvenli Şifreleme Gereksinimleri:

Şifrelemeyi güvenli bir şekilde gerçekleştirmek için karşılanması gereken iki gereksinim vardır. Bunlar:

1. Şifreleme Algoritması: Saldırganın bir veya daha fazla şifreli metne erişimi olsa dahi gizli anahtarı kıramayacak şekilde şifreli metinler üreten çok güçlü bir şifreleme algoritmasına ihtiyaç vardır.

2. Gizli Anahtarı Güvenli Şekilde Paylaşma: Gizli anahtarı, gönderen ile alıcı arasında paylaşmanın güvenli ve sağlam bir yolu olmalıdır. Saldırganın gizli anahtara ulaşamaması gereklidir.

Data Encryption Standard (DES)

DES algoritması, 1970'lerin başında bir IBM ekibi tarafından oluşturulan ve Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) tarafından benimsenen simetrik anahtar blok şifrelemesidir. Algoritma, düz metni 64 bitlik bloklar halinde alır ve bunları 56 bitlik anahtarlar kullanarak şifreli metne dönüştürür. Simetrik bir şifreleme algoritması olduğundan, verinin şifrelenmesinde ve şifresinin çözülmesinde aynı anahtar kullanılır.

DES Algoritması Adımları

Basitçe ifade etmek gerekirse DES, 64 bitlik düz metni alır ve onu 64 bitlik şifreli metne dönüştürür.

Algoritma süreci aşağıdaki adımlardan oluşmaktadır:

1. 64 bitlik düz metin bloğunun bir başlangıç permütasyon (IP) tablosuyla karıştırılmasıyla başlar.

2. Daha sonra, ilk permütasyon (IP) sonucu oluşan permütasyonlu blok iki yarıya bölünür; bunlar Sol Düz Metin (LPT) ve Sağ Düz Metin (RPT) olarak adlandırılır.

3. Her LPT ve RPT, şifreleme işleminin 16 turundan geçerek döngü anahtarlarıyla işlemlere girer.

4. Son adımda LPT ve RPT yeniden birleştirilir ve birleştirilen blokta Son Permütasyon (FP) gerçekleştirilir.

Bu işlemin sonucu istenen 64 bitlik şifreli metni üretir.

Şifreleme işleminin her turunda aşağıdaki aşamalar yer almaktadır:

1. Döngü anahtarı

2. Genişleme permütasyonu

3. S-Box permütasyonu

4. P-Box permütasyonu

5. XOR ve yer değiştirme (her turda LPT VE RPT yer değiştirmektedir.)

Şifre çözme işlemi için aynı algoritma üzerinde döngü anahtarlarının ters sırada kullanılması yeterlidir.

DES'İN ZAYIFLIKLARI

DES algoritması ilk oluşturulduğunda ve standartlaştırıldığında, o nesil bilgisayarlar için gerçekten çok güçlü bir şifreleme algoritmasıydı. Fakat bilgisayarların gelişmesiyle birlikte DES algoritmasını kırmak, aşağıdaki resimde görüldüğü gibi her geçen yıl daha kolay ve hızlı hale geldi.

Chronology of DES Cracking	
Broken for the first time	1997
Broken in 56 hours	1998
Broken in 22 hours and 15 minutes	1999
Capable of broken in 5 minutes	2021

Source: Wikipedia

DES'in çok iyi tasarlanmış bir blok şifre olduğu kanıtlanmıştır. Kapsamlı anahtar arama saldırıları dışında DES'e yönelik önemli bir kriptanaliz saldırısı gerçekleşmemiştir.

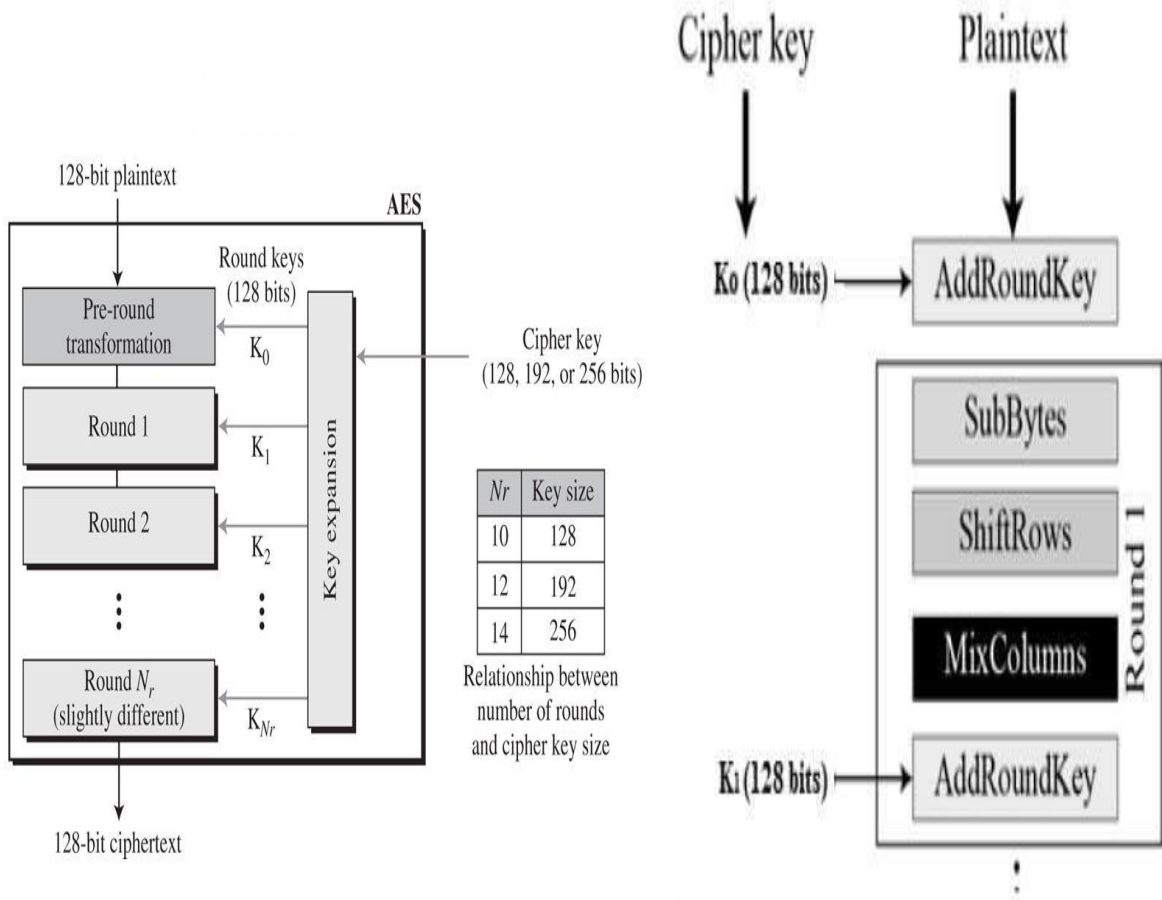
Bu sebeple daha uzun anahtar boyutları kullanan daha sağlam bir algoritmaya ihtiyaç duyuldu. Bu sorunu çözmek için Triple DES oluşturuldu ancak nispeten yavaş bir algoritma olması nedeniyle hiçbir zaman ana akım haline gelmedi. Bu dezavantajın üstesinden gelebilmek için Advanced Encryption Standard (AES) ortaya çıktı.

Advanced Encryption Standard (AES)

Gelişmiş Şifreleme Standardı (AES), ABD Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) tarafından 2001 yılında oluşturulan elektronik verilerin şifrlenmesine yönelik bir şifreleme standartıdır. AES, DES'ten çok daha güçlüdür, günümüzde yaygın olarak kullanılmaktadır.

- AES bir blok şifrelemedir.
- Anahtar boyutu 128/192/256 bit olabilir.
- Verileri 128 bitlik bloklar halinde şifreler.

Algoritmanın çalışma şeması



AES'İN GÜVENLİĞİ VE AVANTAJLARI

Günümüz kriptografisinde AES, hem donanım hem de yazılımda yaygın olarak benimsenmekte ve kullanılmaktadır. Bugüne kadar AES'e karşı pratik bir kriptanaliz saldırısı keşfedilmemiştir. Ek olarak, AES'e karşı kapsamlı anahtar aramaları (bruteforce) gerçekleştirme becerisindeki ilerlemeye karşı 'geleceğe hazır' olma olanağı sağlayan daha uzun anahtar uzunluğu esnekliğine sahiptir.

Ancak tıpkı DES'te olduğu gibi, AES güvenliği de yalnızca doğru şekilde uygulandığında ve iyi bir anahtar yönetimi gerçekleştirildiğinde sağlanabilir.

Temel Prensiplerin Belirlenmesi:

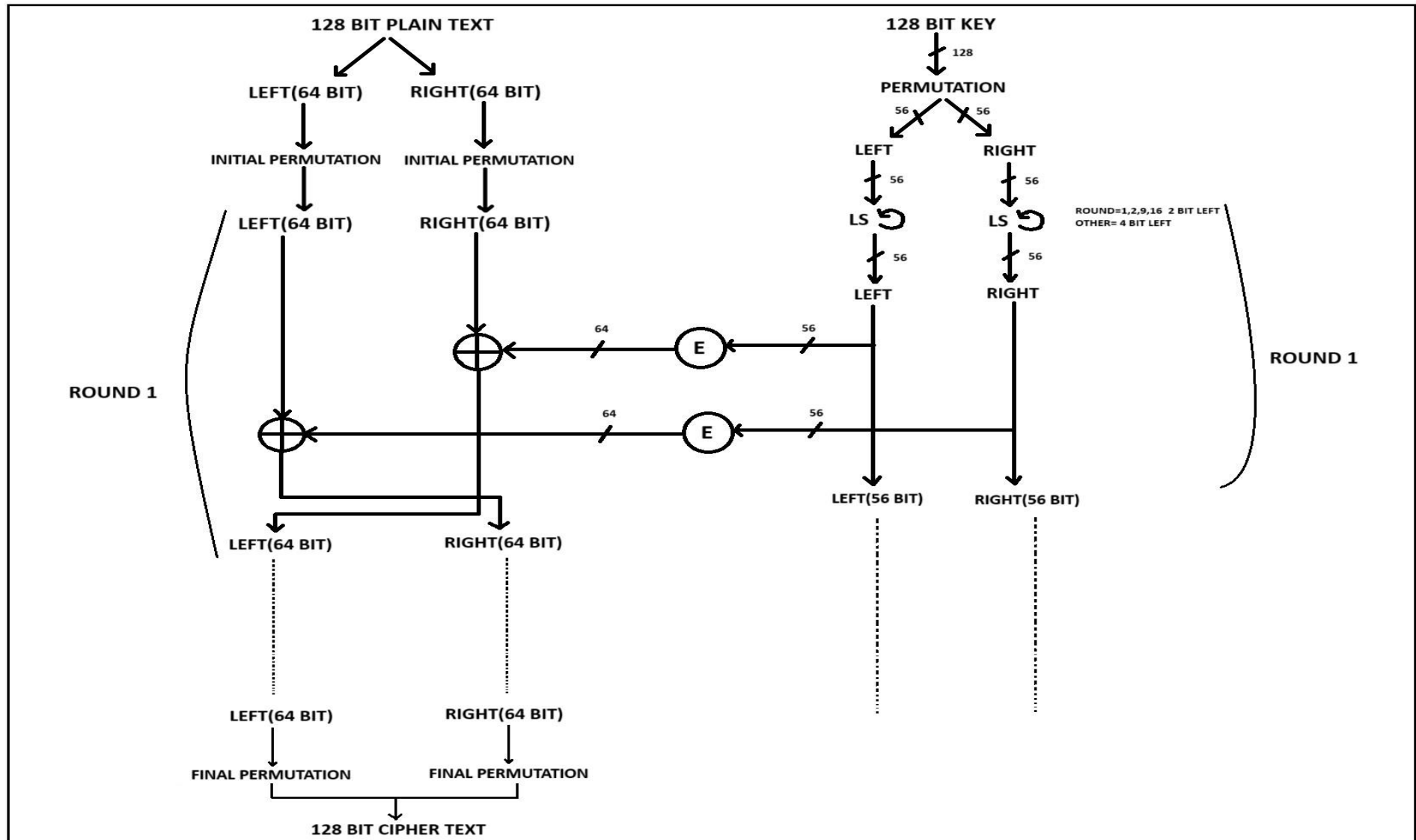
Şifreleme algoritması olarak simetrik blok şifreleme oluşturmak amaçlanmıştır. Tasarlanan algoritma DES şifreleme algoritmasından esinlenerek oluşturulmuştur. Şifrelenecek metin 128 bitlik bloklar halinde şifrelenir. Anahtar boyutu 128 bit olarak belirlenmiştir. Algoritmamız birbirini takip eden 16 turdan oluşmaktadır.

Algoritmanın Tasarlanması:

Tasarlanan şifreleme algoritması sırasıyla aşağıdaki adımlardan oluşmaktadır:

1. Şifrelenecek metin 128 bitlik bloklar halinde şifrelenir.
2. Blok'ta eksik bit bulunması durumunda padding işlemi(doldurma) uygulanarak blok boyutu 128 bite tamamlanır.
3. 128 bitlik blok ilk olarak 64 bitlik sağ ve sol 2 parçaya ayrılır.
4. 64 bitlik sağ ve sol parçaya başlangıç permütasyonu uygulanarak bitlerin konumları değiştirilerek, karıştırma işlemi uygulanır.
5. Şifrelemede kullanılacak anahtar 128 bit uzunluğundadır.
6. 128 bitlik anahtar bir karıştırma tablosu yardımıyla karıştırılarak, 112 bite düşürülür (Parite bitleri çıkarılıyor).
7. 112 bitlik bu anahtar sağ ve sol olarak 2 kısıma ayrılır.
8. Anahtarın sağ ve sol kısmı 1, 2, 9, 16. turlarda 2 bit sola, diğer turlarda 4 bit sola kaydırılarak döngü anahtarları oluşturulur.
9. Oluşturulan döngü anahtarının sağ ve sol kısmı, bir genişletme tablosu yardımıyla 56 bitten 64 bite genişletilir.
10. Genişletme işlemi sonucunda oluşan 64 bitlik, döngü anahtarının sağ kısmı ile şifrelenecek metnin sol kısmı xor'lanarak oluşan bit dizesi ikinci turun sağ kısmına yazılır.
11. Genişletme işlemi sonucunda oluşan 64 bitlik, döngü anahtarının sol kısmı ise şifrelenecek metnin sağ kısmı ile xor'lanarak oluşan bit dizesi ikinci turun sol kısmına yazılır.
12. Bu şekilde bir tur tamamlanmış olacaktır, algoritmamız toplamda 16 turdan oluşmaktadır.
13. 16 turun sonunda oluşan, şifrelenecek metnin sağ ve sol kısmına final permütasyonu uygulanarak şifreli metin oluşturulur ve işlemler tamamlanır.
14. Şifre çözme işlemlerinde ise döngü anahtarlarının ters sırada uygulanması sonucunda şifrelenmiş metinden orijinal metin elde edilir.

ALGORİTMAYA AİT AKIŞ ŞEMASI



ALGORTİMANIN KODLANMASI SONUCU OLUŞAN ÇIKTILAR

```
C:\Windows\system32\cmd. x + v
C:\Users\İbrahim ATAŞ\Desktop>python bsm465_kriptlojiyegiris.py
Sifrelenecek metni girin(lutfen turkce karakterler girmeyiniz): Data Encryption Standard (DES) is a block cipher with a
56-bit key length that has played a significant role in data security. Data encryption standard (DES) has been found vul
nerable to very powerful attacks therefore, the popularity of DES has been found slightly on the decline. DES is a block
cipher and encrypts data in blocks of size of 64 bits each, which means 64 bits of plain text go as the input to DES, w
hich produces 64 bits of ciphertext. The same algorithm and key are used for encryption and decryption, with minor diffe
rences. The key length is 56 bits.
Anahtar metni girin(16 adet karakter girilmelidir, lutfen turkce karakterler girmeyin!): key0123456789key

Şifrelenmiş Metin: f0b52333f2d74ef46491be7f7962bfdca2e41702c89100bd7384ab703d46a3dbe9ec302eebd045a653d0ab3e3b4bbbedcb7fa7
e25f2cc00bf0087a36a3107b09feaec272ffacc00bc4589ea723c49b6cbe6ec3267e8d147ba4183ea6e3546a8daf0a33f22bbd14ef44996a37d3849a
59ff7be3a33e29600904491be7f7954b4dcfbbc272ef4d600a74184ab3e3c49b2cdaa881614b29848b55491a47a3855b59fedb93d23bbce55b853d0a
87b3c49f1d9f6a37331feca59f44e95b87f3b4bb49fa2ad2733fadb4ba7509fbd7b2b41a4d3f0a97f67efd045f40084a27b2b42b7d0f6b57328fd986
491509fba6b3546a3d6e7a27321f4cd4eb073d0a27f2a07b3dafbec3c29bbcc48b10083a6773e4fa5d3accec1702c89849a70094af7d354ebfdaa2af3
a37f3dd52f40091ea7c3548b2d4fbbc2734bbdc41a0419eae3e3c49b2cde1a72067f4de00a741d0a3707945bdd0b6ec312eefcb00b1498aa3e3641f
189e1a4732afed94ea74193a2327950b9d6a2a33567ebd441bd00c6fe3e3b4ea5ccedec3234bbcc48b14ed0be7b2153f1d8edec1702c89400a30099a
46e2c53f1cbe6b93022e89816e04899a9767957a3d0a2af3a37f3dd52a00092a36a2a07bed9a2bf322afe9841b84588be307973b9dae3a23767f0dd5
9f4479fb8772d4fbc9fa2aa3c35bbdd4eb74182af3e2c54b4dbe3a23767ffdd43a65289ba6a3048bf9ff5a5272fbbd549ba5980be773649fd9ff0a93
d24fecb0ef44f82ea7a3041b7daeea93d20efd000bd7498af3e3242a89ff1e255419dbe26d253d0ff287945b8cb
Şifreleme işlemi 0.05010843276977539 saniyede gerçekleşti.

Şifresi çözümlenmiş metin: Data Encryption Standard (DES) is a block cipher with a 56-bit key length that has played a s
ignificant role in data security. Data encryption standard (DES) has been found vulnerable to very powerful attacks ther
efore, the popularity of DES has been found slightly on the decline. DES is a block cipher and encrypts data in blocks o
f size of 64 bits each, which means 64 bits of plain text go as the input to DES, which produces 64 bits of ciphertext.
The same algorithm and key are used for encryption and decryption, with minor differences. The key length is 56 bits.
Şifre çözme işlemi 0.0500028133392334 saniyede gerçekleşti.
```


KAYNAKLAR

- <https://www.geeksforgeeks.org/symmetric-cipher-model/>
- <https://www.simplilearn.com/what-is-des-article>
- https://acikders.ankara.edu.tr/pluginfile.php/126028/mod_resource/content/1/Understanding_Cryptography_Chptr_3--DES.pdf
- <https://www.geeksforgeeks.org/data-encryption-standard-des-set-1/>
- <https://furkan-dvlp.medium.com/des-%C5%9Fi%CC%87freleme-algori%CC%87tmasi-64edae838ef3>
- https://en.wikipedia.org/wiki/Data_Encryption_Standard
- https://en.wikipedia.org/wiki/Advanced_Encryption_Standard
- <https://www.javatpoint.com/what-is-aes>
- https://www.tutorialspoint.com/cryptography/advanced_encryption_standard.htm
- <https://www.geeksforgeeks.org/advanced-encryption-standard-aes/>