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

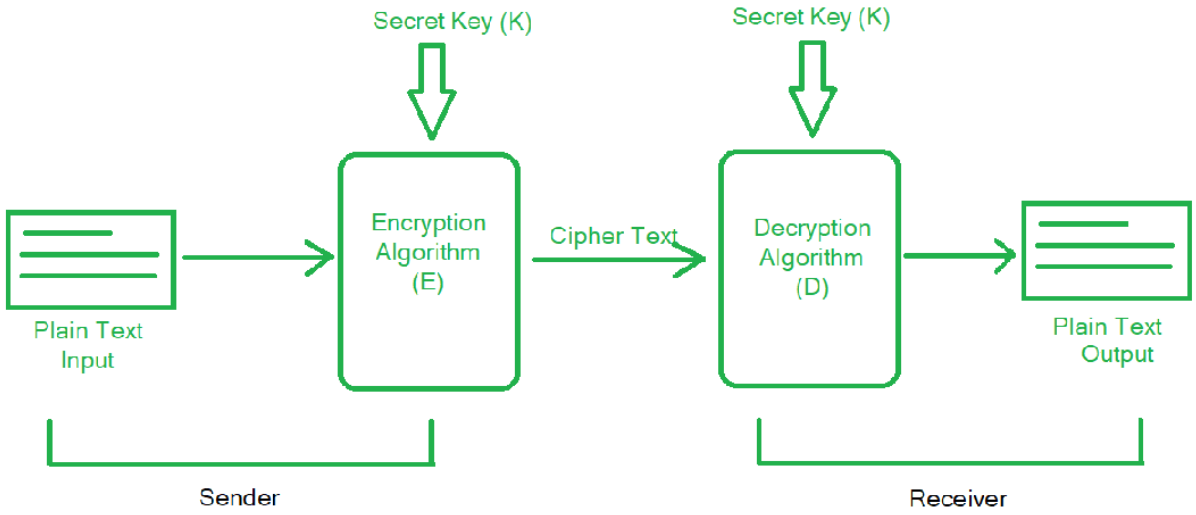
Simetrik Şifreleme, şifrelemenin en temel ve eski yöntemidir. Verilerin hem şifrelenmesi hem de şifresinin çözülme işlemi için yalnızca gizli bir anahtar kullanır. Bu nedenle Tek Anahtarlı Şifreleme olarak da bilinir.

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 kriptoanaliz saldırısı gerçekleşmemiştir.

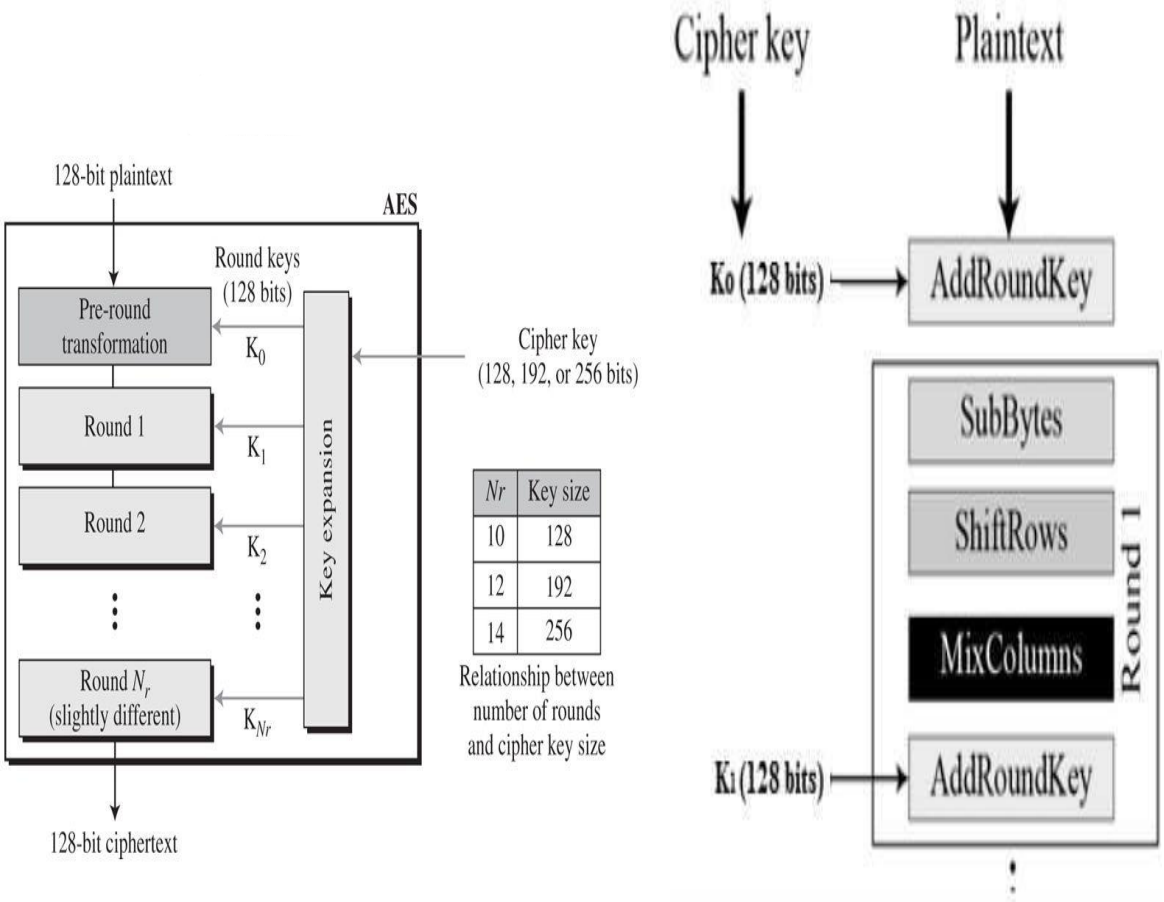
Bu sebeple daha uzun anahtar boyutları kullanan daha sağlam bir algoritmaya ihtiyaç duyuldu. Bu sorunu çözmek için Triple DES oluşturuldu ancak nispeten yavaş bir algoritma olması nedeniyle hiçbir zaman ana akım haline gelmedi. Bu dezavantajın üstesinden gelebilmek için Advanced Encryption Standard (AES)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

Advanced Encryption Standard (AES)

Gelişmiş Şifreleme Standardı (AES), ABD Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) tarafından 2001 yılında oluşturulan elektronik verilerin şifrelenmesine 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 kriptoanaliz saldırısı keşfedilmemiştir. Ek olarak, AES'e karşı kapsamlı anahtar aramaları(brutte-force) 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:

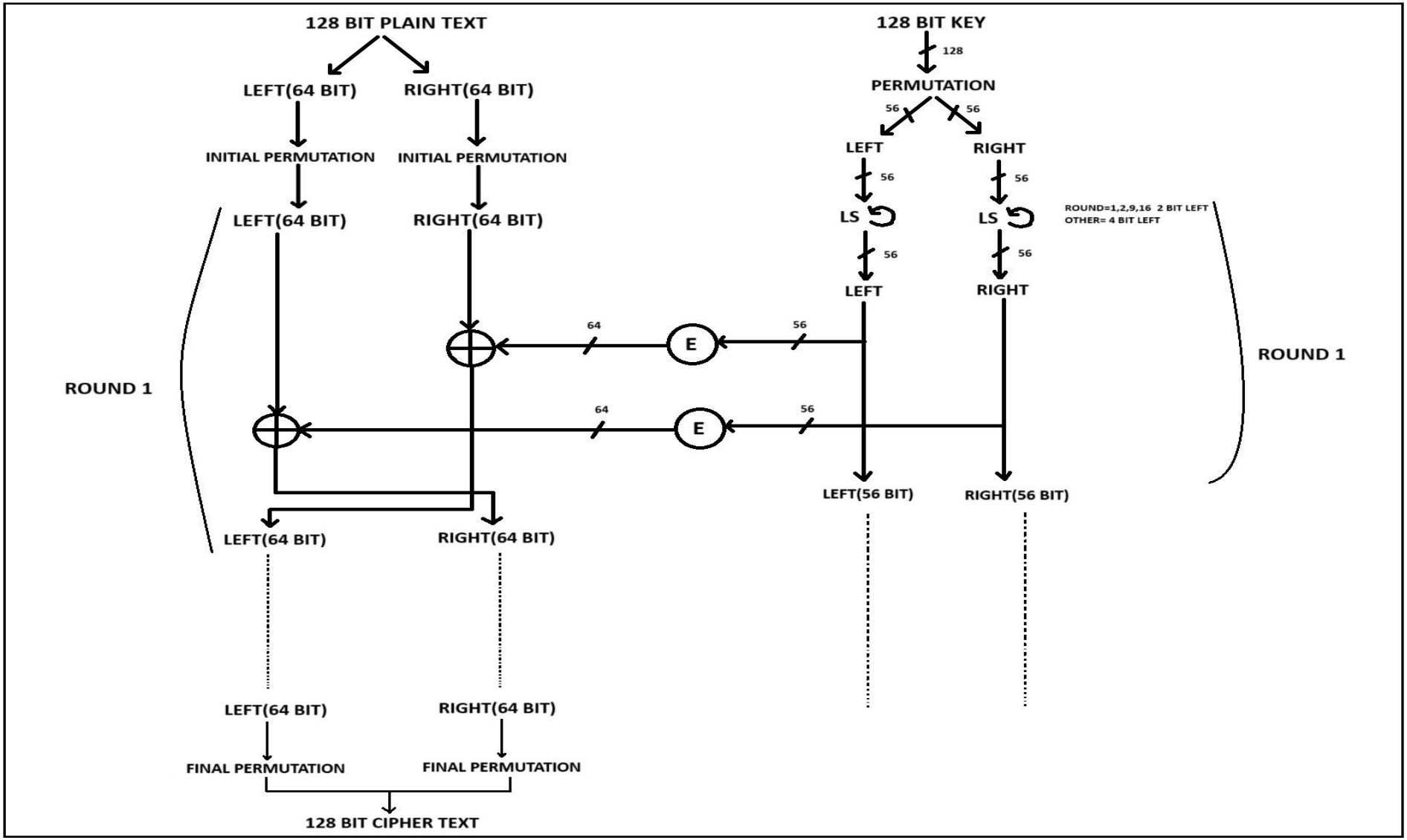
Şifreleme algoritması olarak simetrik blok şifreleme oluşturmak amaçlanmıştır. Tasarlanan algoritma DES şifreleme algoritmasından esinlenerek oluşturulmuştur. Şifrelenecek metin 128 bitlik bloklar halinde şifrelenir. Anahtar boyutu 128 bit olarak belirlenmiştir. Algoritmamız birbirini takip eden 16 turdan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

Algoritmanın Tasarlanması:

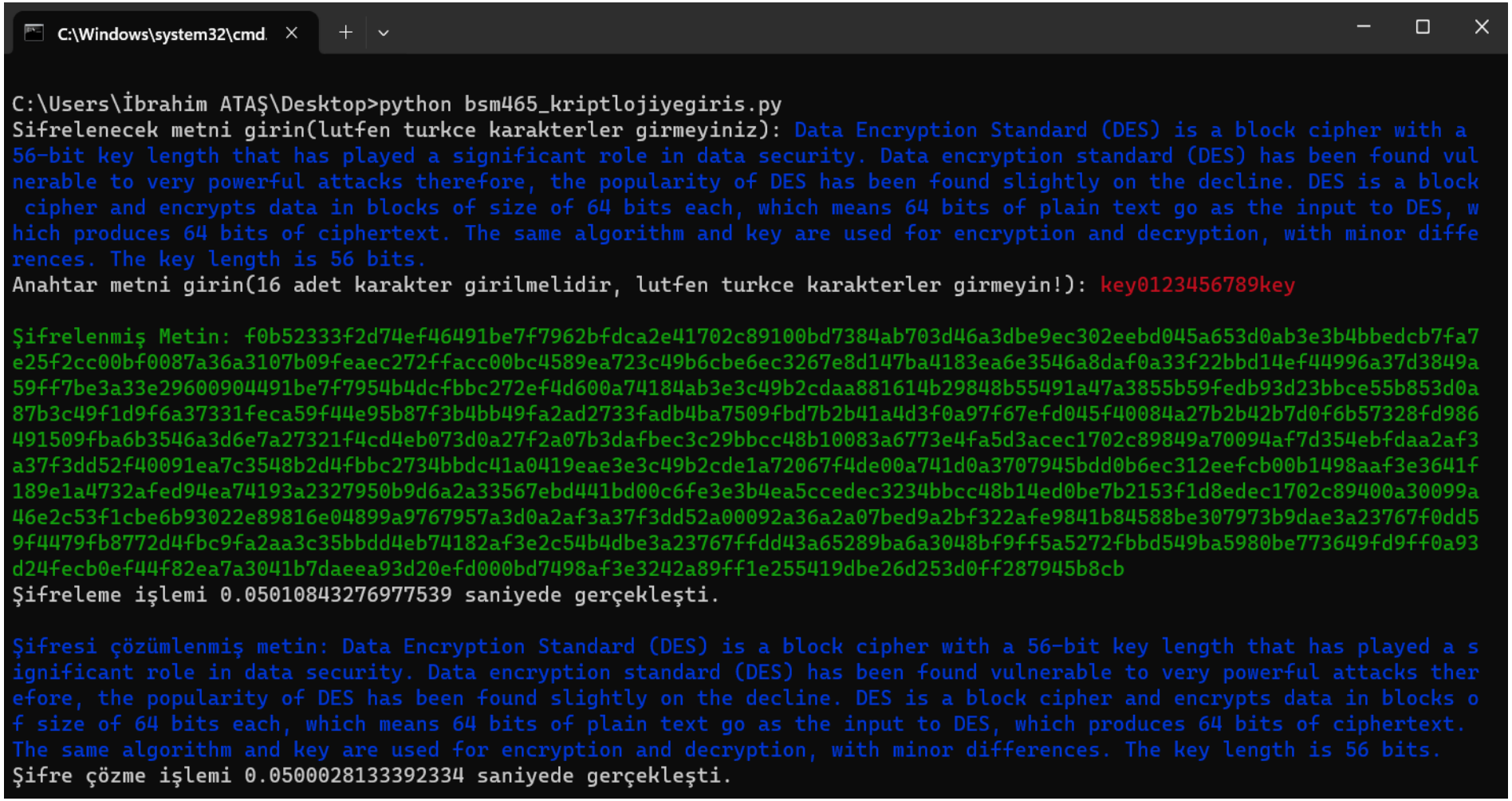
Tasarlanan şifreleme algoritması sırasıyla aşağıdaki adımlardan oluşmaktadır:

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 kısma 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



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/