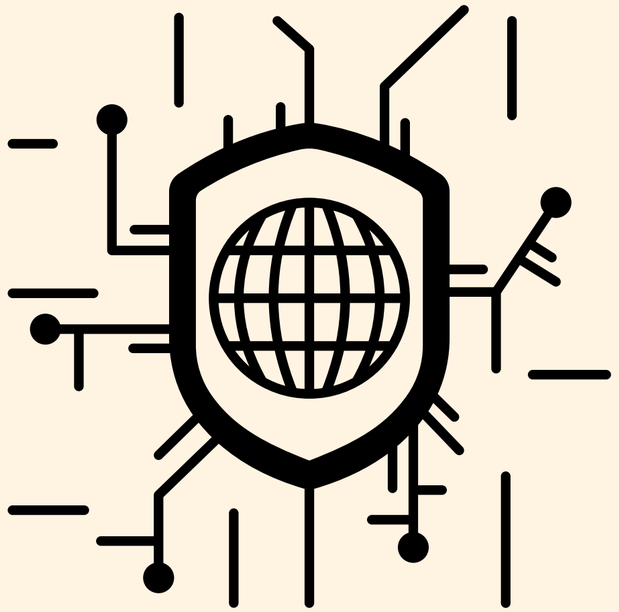
AĞ GÜVENLİĞİ

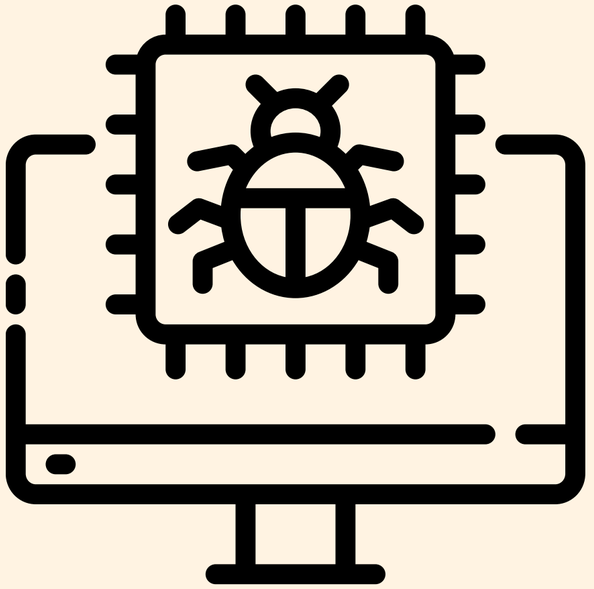
AES ALGORİTMASI

HAZIRLAYANLAR

İSMAİL KARAÇAYIR-G201210303

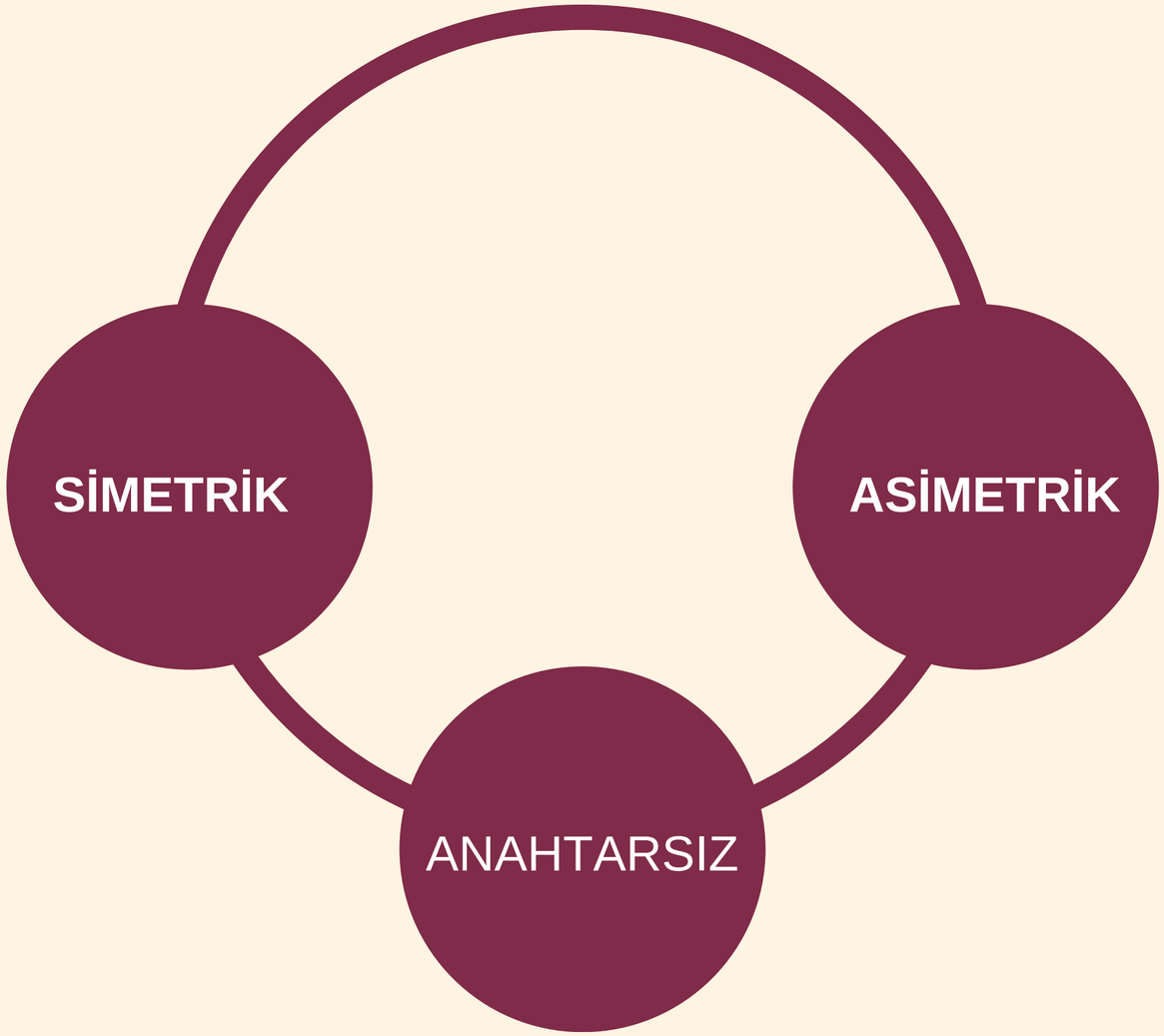
2/A





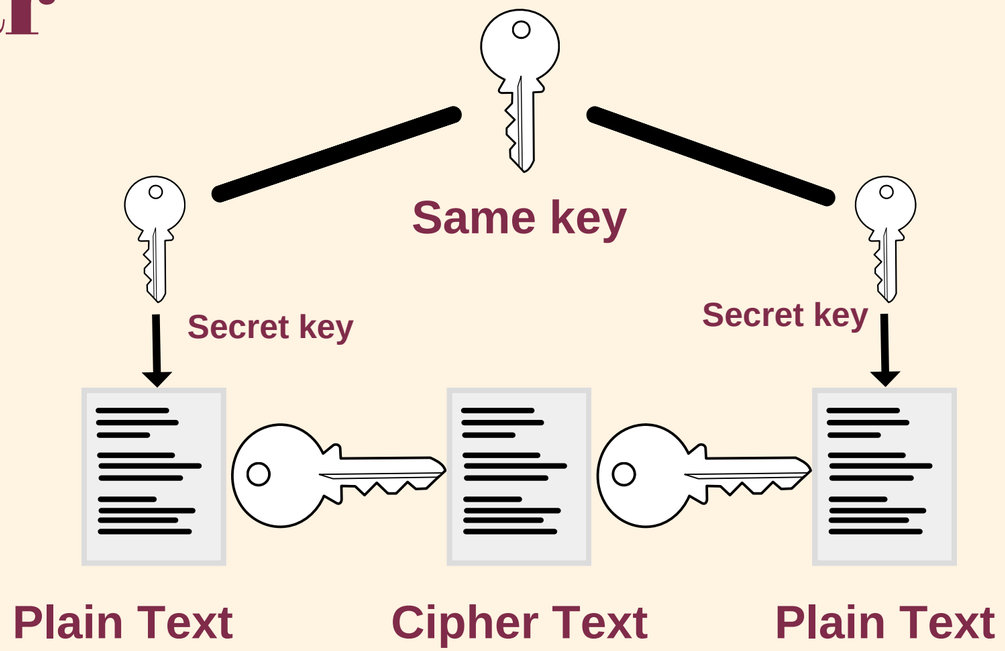
Kriptografik sistemler

Kriptografi ya da 'şifreleme' okunabilir durumdaki bir verinin içerdiği bilginin istenmeyen taraflarca anlaşılamayacak bir hale dönüştürülmesinde kullanılan yöntemlerin tümüdür. Kriptografi bir matematiksel yöntemler bütünüdür ve önemli bilgilerin güvenliği için gerekli gizlilik, aslıyla aynılık, kimlik denetimi, ve asılsız reddi önleme gibi şartları sağlamak amaçlıdır.



Simetrik Anahtarlı Algoritmalar

Simetrik şifreleme, bilgileri şifrelemek ve deşifre etmek için yalnızca bir gizli anahtar içeren şifreleme türüdür. Simetrik şifreleme, kriptografi teknikleri ve şifreleme algoritmaları içinde en eski ve en iyi bilinen tekniktir. Bir sayı, bir kelime veya rastgele harfler dizisi olabilen gizli bir anahtar kullanır. Gönderen ve alıcı, tüm mesajları şifrelemek ve şifresini çözmek için kullanılan gizli anahtarı bilmelidir. İşlem süresinin hızlı olması simetrik şifreleme algoritmalarının en önemli avantajlarındandır. Blowfish, **AES**, RC4, DES, RC5 simetrik şifrelemeye örnektir.



Simetrik Anahtarlı Algoritmalar-DEVAM

Avantajları

- Şifreleme ve şifreyi çözme işlemleri hızlıdır, donanımla gerçekleştirilmesi kolaydır.
- Taraflar arasındaki iletişimin gizliliği sağlanır.
- Verinin bütünlüğü sağlanır. Şifreli metin çözülemedikçe orijinal metin değiştirilemeyecektir.

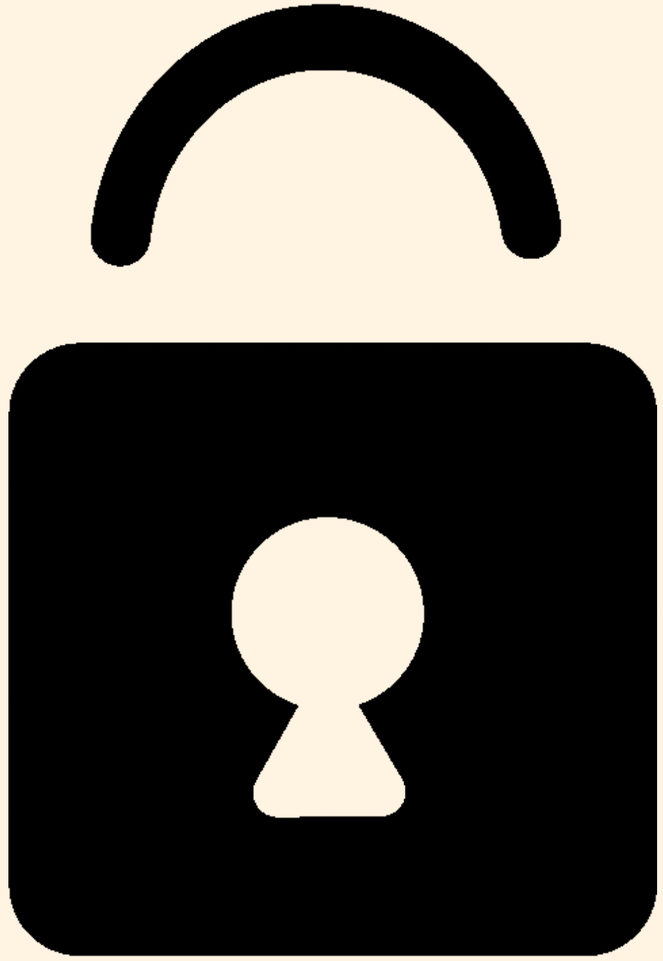
Simetrik Anahtarlı Algoritmalar-DEVAM

Dezavantajları

- Anahtar saklamak zordur..
- Güvenilir anahtar dağıtımı zordur.
- Bütünlük sağlamaz. Ortadaki bir kişi tarafından veri değiştirilmiş olabilir.
- Kimlik doğrulama ve bütünlük sağlamadığı için inkar edilememezlik sağlamaz.

AES ALGORİTMASI

1997 yılına kadar veri şifreleme standardı olarak DES Algoritması kullanılıyordu. Gelişen teknoloji ile birlikte DES Algoritmasının 64 bitlik anahtar uzayı güvenilirliğini yitirmeye başladı. Bu sebeple NIST (Ulusal Standartlar ve Teknoloji Enstitüsü) 1997 yılında yeni bir yarışma düzenlemiştir.Joan Daemen ve Vincent Rijmen tarafından tasarlanan Rijndael Algoritması Advanced Encryption Standard (AES) ismiyle NIST tarafından kabul edilmiştir.



AES ALGORİTMASI-DEVAM

- Hem şifreleme hem şifre çözme işlemleri için aynı anahtar kullanılır. AES için girdi ve çıktı matrisleri her zaman 128 bit olmak zorundadır ancak anahtar uzunluğu 128, 192 veya 256 bit olabilir.
- Tablo 1.3.2.1 ile gösterilen durum matrisinde her bir hücre 8 bit yer kaplamaktadır, 16 hücre bulunduğu için toplam 128 bitlik bir veriye karşılık düşer. Şifrelenecek mesaj ve anahtar durum matrisleri şeklinde düşünülerek üzerlerinde gerekli işlemler yapılır.

S0	S4	S8	S12
S1	S5	S9	S13
S2	S6	S10	S14
S3	S7	S11	S15

Tablo 1.3.2.1. Durum Matrisi

AES ALGORİTMASI AŞAMALARI

AES algoritması Bayt Değiştirme, Satır Kaydırma, Sütun Karıştırma ve Tur Anahtarı ile Toplama gibi adımların tekrar etmesi şeklinde düşünülebilir.

Bayt Değiştirme

Bayt değiştirme işlemi durum matrisindeki baytların farklı baytlara dönüştürülmesi işlemidir. Bu dönüşüm daha önceden belli bir lookup table üzerinden yapılır. Örnek bir tablo yanda verilmiştir.

0x48	0xf6	0x24	0x5b		0x52	0x42	0x36	0x39
0xcc	0x1a	0xb7	0x34		0x4b	0xa2	0xa9	0x18
0x37	0xc9	0xd4	0x71		0x9a	0xdd	0x48	0xa3
0x1a	0x67	0x33	0x01		0xa2	0x85	0xc3	0x7c

AES ALGORİTMASI AŞAMALARI-DEVAM

Satır Kaydırma

Satır kaydırma işlemi bayt değiştirme işleminden sonra oluşan yeni durum üzerine uygulanır. Durum matrisindeki satırların belli değerde sola kaydırılması anlamına gelir.

				Kaydır				
0x48	0xf6	0x24	0x5b	0 bayt	0x48	0xf6	0x24	0x5b
0xcc	0x1a	0xb7	0x34	1 bayt	0x1a	0xb7	0x34	0xcc
0x37	0xc9	0xd4	0x71	2 bayt	0xd4	0x71	0x37	0xc9
0x1a	0x67	0x33	0x01	3 bayt	0x01	0x1a	0x67	0x33

AES ALGORİTMASI AŞAMALARI-DEVAM

Sütun Karıştırma

Sütun karıştırma işlemi satır karıştırma adımında oluşan durum matrisinin her sütunun ayrı ayrı belli bir matris ile çarpılması ve ortaya çıkan matrisin yeni sütun olarak kullanılmasıdır.

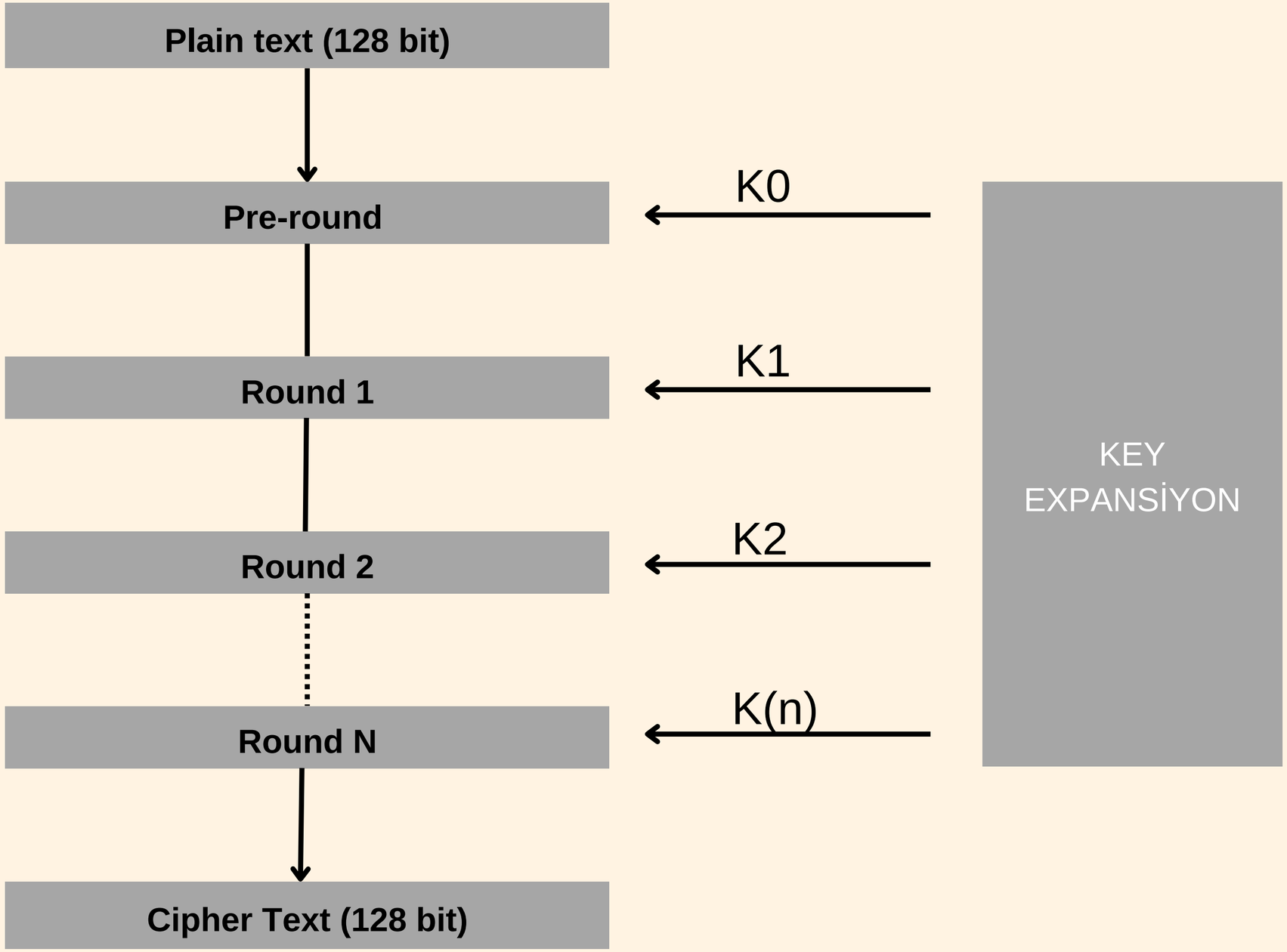
0x02	0x03	0x01	0x01		S0	S0’
0x01	0x02	0x03	0x01	·	S1	= S1’
0x01	0x01	0x02	0x03		S2	S2’
0x03	0x01	0x01	0x02		S3	S3’

AES ALGORİTMASI AŞAMALARI-DEVAM

Tur Anahtarı ile Toplama

Her turun sonunda bulunan mesaj o anki tur anahtarı ile toplanır. Her turda farklı bir anahtar kullanıldığı için tur sayısı kadar yeni anahtar gereklidir. Yanda 10 turluk bir AES 128 algoritmasında gerekli anahtar tablosunun bir kısmı gösterilmiştir.

0	1	2	3	4	5	6	7		42
0x61	0x74	0x6c	0x6b	0xf2	0x86	0xea	0x81	……..	0xa3
0x79	0x61	0x65	0x74	0x80	0xe1	0x84	0xf0	……..	0x39
0x73	0x74	0x63	0x69	0x8a	0xfe	0x9d	0xf4	……..	0x4c
0x65	0x69	0x69	0x69	0x1a	0x73	0x1a	0x73	……..	0x67


Plain text (128 bit)
Pre-round
Round 1
Round 2
Round N
Cipher Text (128 bit)
K0
K1
K2
K(n)
KEY
EXPANSİYON

AES ALGORİTMASI AŞAMALARI-DEVAM

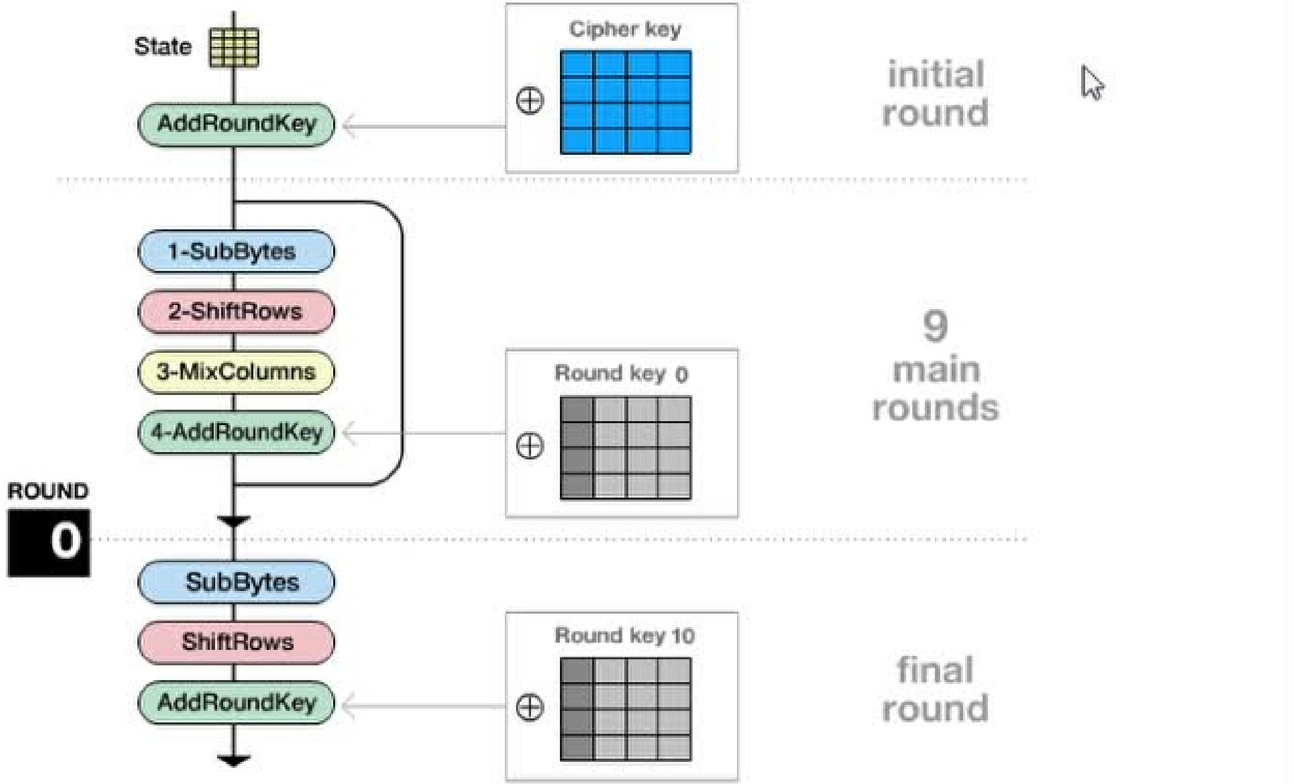
Tur Anahtarının Üretilmesi

Tur anahtarlarının üretilip sıralı bir şekilde bir bellek alanına yazılmasıyla oluşan diziye genişletilmiş anahtar dizisi denir

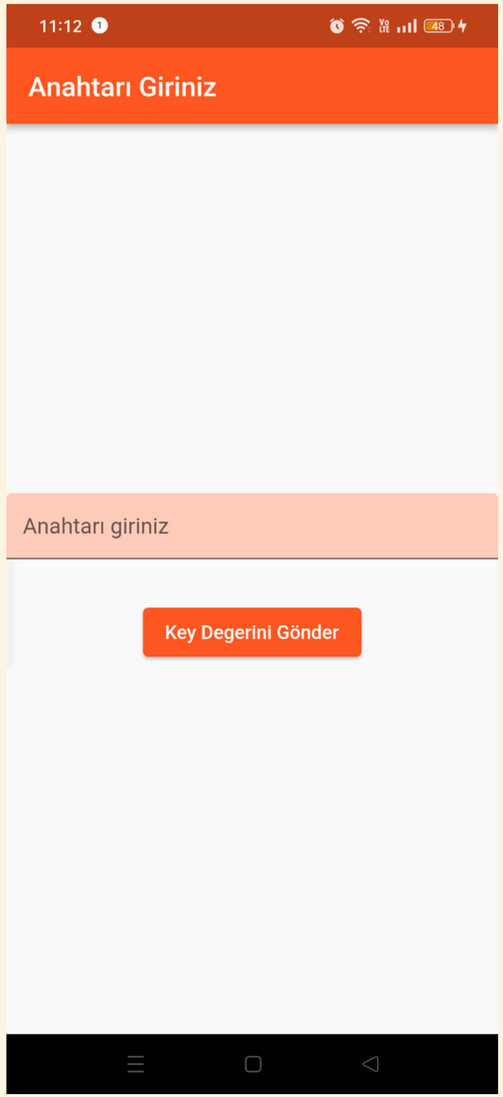
Deşifreleme

Ters Bayt Değiştirme, Ters Satır Kaydırma, Ters Sütun Karıştırma ve Tur Anahtarıyla Toplama adımlarını içerir ancak Tur Anahtarıyla Toplama adımı genişletilmiş anahtarın içerisindeki son anahtardan başlayarak geriye doğru ilerler. Yani şifreleme için kullandığımız son anahtar deşifreleme için kullandığımız ilk anahtar olur.

Encryption Process



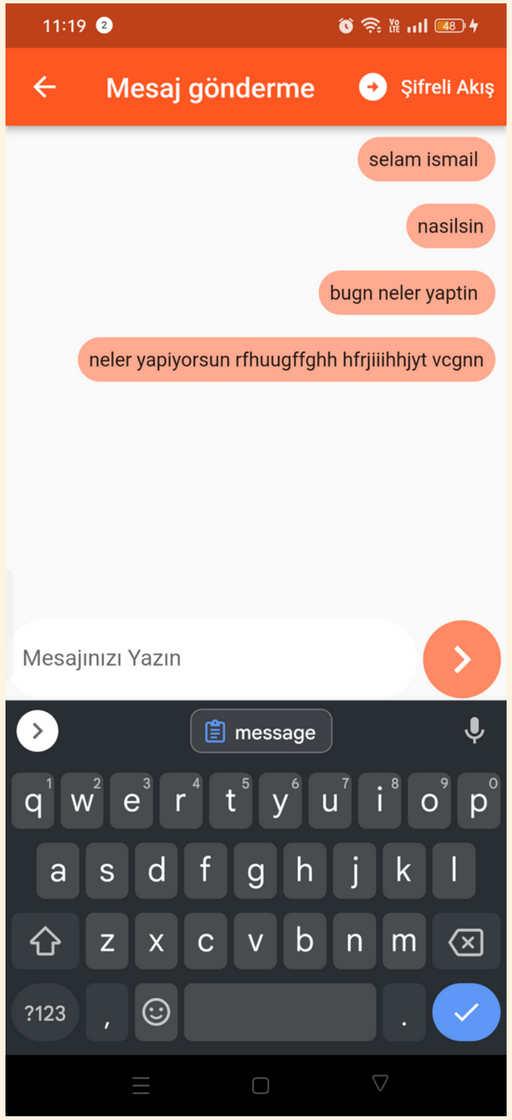
AES ALGORİTMASI -PROJE GÖRSELLERİ



Kullanıcıdan Anahtar Alınması

Kullanıcıdan alınan anahtar değeri (uzunluğu ne olursa olsun)
128 bit haline getirilmek için fonksiyona yollanır (128 bit den uzunsa 128 e indirilir 128 bitden kısa ise dolgu bitti eklenir)

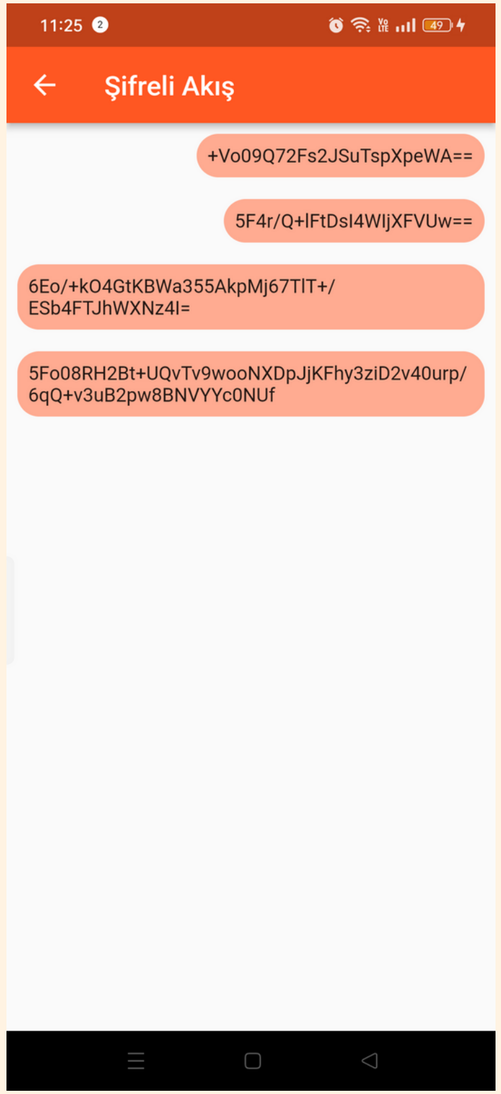
AES ALGORİTMASI -PROJE GÖRSELLERİ



Şifre Çözülme

Kullanıcıdan alınan text değeri şifrelenerek (AES) firestore veritabanı na kayıt edilir . Stream yapısı ile dinlenen tablo , veritabanından alınan şifreli veri şifre çözme işlemi yapılarak arayüz de gösterilir.

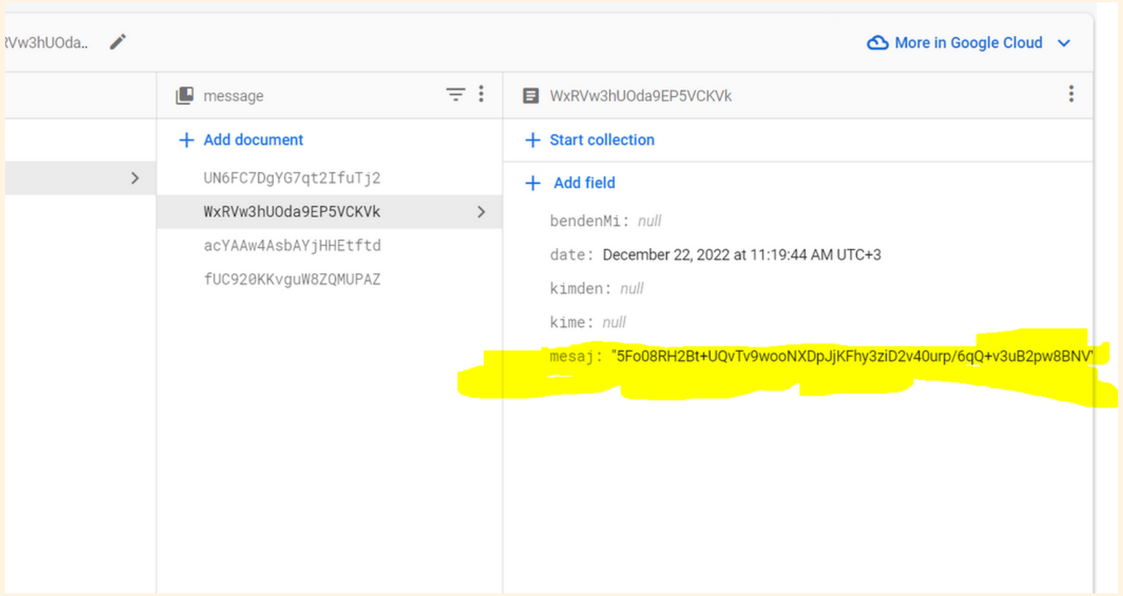
AES ALGORİTMASI -PROJE GÖRSELLERİ



Şifreli Akış

Kullanıcıdan alınan text değeri şifrelenerek şifreli akış sayfasında gösterilmesi (veritabanından çekiliyor)

AES ALGORİTMASI -PROJE GÖRSELLERİ



Veritabanı

Veritabanına mesajlar şifreli bir şekilde ekleniyor ,böylece uçtan uça şifreleme gerçekleşmiş oluyor

KAYNAKÇA

- https://medium.com/@yavuzunver/aes
- https://www.geeksforgeeks.org
- https://www.youtube.com/watch?v=q0WccRi5t4M
- https://khosann.com/kriptografi-101
- https://stackoverflow.com/