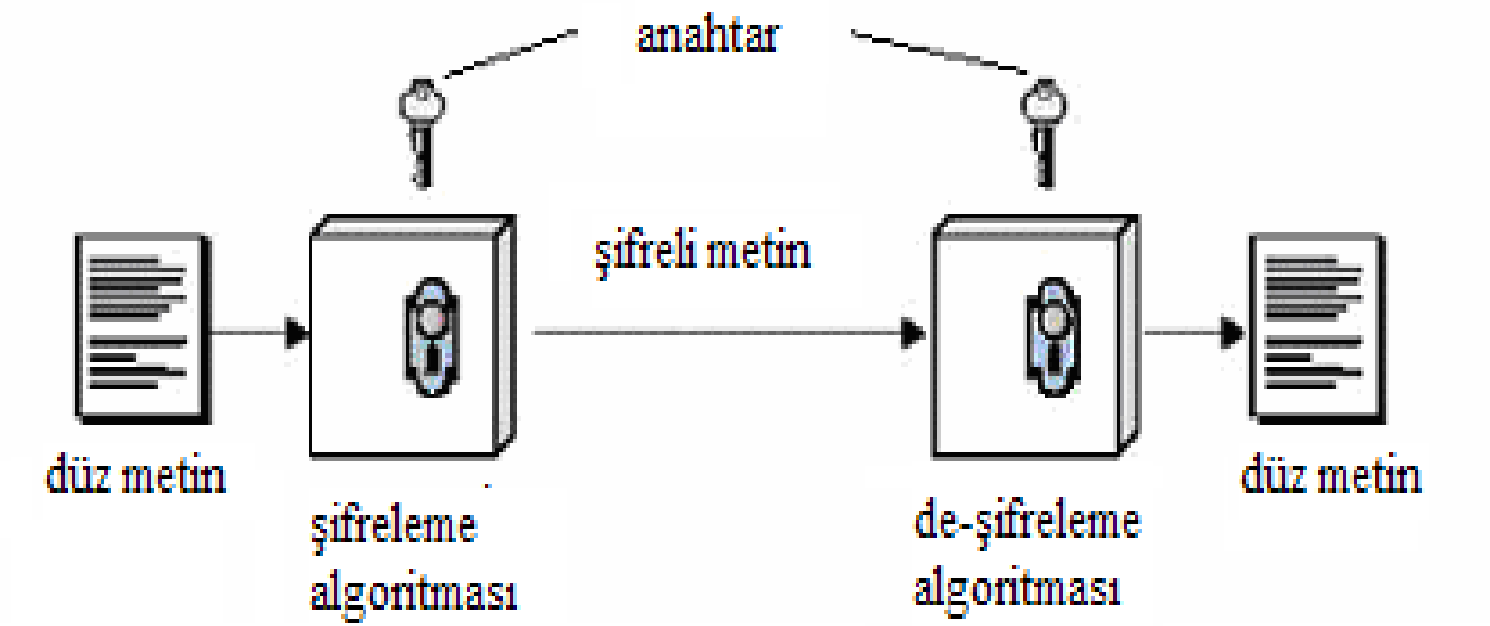
ŞİFRELEME YÖNTEMLERİ

GİRİŞ

- Şifreleme bir mesajın gizliliğini sağlamak için kullanılan bir yöntemdir. Şifreleme çeşitlerinden biri olan simetrik şifrelemede ise amaç gönderici ile alıcının ortak bir anahtar üzerinde ve ortak bir şifreleme ile deşifreleme algoritması üzerinde anlaşıp, mesajı diğer kişilerden korumaktır.
- Simetrik şifrelemede beş bileşen bulunmaktadır. Bu bileşenler ve şifreleme işleminin nasıl yapıldığı Şekil 1'de gösterilmektedir.
- Simetrik şifrelemede güvenliği sağlayan anahtardır. Çünkü gizli olan tek şey anahtardır, şifreleme ve deşifreleme algoritmaları herkese açıktır. Farklı anahtarlar sayesinde aynı mesaj ve aynı algoritma ile birbirinden bağımsız şifreli metinler üretilebilir.

- Simetrik şifreleme yöntemleri metin üzerindeki işlemlerine göre iki grup altında sınıflandırılabilir. Bunlardan biri karakter tabanlı yani geleneksel şifreleme sistemleri (Monoalfabetik ve polialfabetik) ve diğeri ise bit tabanlı şifreleme yani modern şifreleme sistemleridir.



Bit Tabanlı Şifreleme Sistemleri

- **1-DES (Data Encryption Standard) :** Dünyada en yaygın kullanılan şifreleme algoritmalarından birisidir. DES, IBM tarafından geliştirilmiştir. 1975 yılında “Federal Register” tarafından yayınlanmıştır. DES 64 bitlik veriyi 56 bitlik anahtar kullanarak şifreler [2]. Ayrıca klasik Feistel Ağı kullanılarak [3] temelde şifreleme işleminin deşifreleme işlemiyle aynı olması sağlanmıştır. Kullanılan teknikler yayılma ve karıştırmadır. DES’in en büyük dezavantajı anahtar uzunluğunun 56 bit olmasıdır. 1975 yılında yayınlanan bu algoritma günümüzde geliştirilen modern bilgisayarlar tarafından yapılan saldırılar karşısında yetersiz kalmaktadır. Daha güvenli şifreleme ihtiyacından dolayı DES, Triple-DES olarak geliştirilmiştir. Triple -DES algoritması geriye uyumluluğu da desteklemek amacıyla 2 adet 56 bitlik anahtar kullanır. Triple-DES algoritması, DES algoritmasının şifreleme, deşifreleme, şifreleme şeklinde uygulanmasıdır.

- **2-TWOFISH :** 1998 yılında yayınlanan bu algoritma Bruce Schneier - John Kelsey - Doug Whiting - David Wagner - Chris Hall - Niels Ferguson tarafından yaratılmış ve analiz edilmiştir [4]. AES finalistlerinden biridir ve AES kadar hızlıdır. Aynı DES gibi Feistel yapısını kullanır. DES'den farklarından biri anahtar kullanılarak yaratılan değişken S-box (Substitution box – Değiştirme kutuları)' lara sahip olmasıdır. Ayrıca 128 bitlik düz metni 32 bitlik parçalara ayırarak işlemlerin çoğunu 32 bitlik değerler üzerinde gerçekleştirir. AES'den farklı olarak eklenen 2 adet 1 bitlik rotasyon, şifreleme ve deşifreleme algoritmalarını birbirinden farklı yapmış, bu ise uygulama maliyetini arttırmış, aynı zamanda yazılım uygulamalarını %5 yavaşlatmıştır

- **3-IRON :** Diğer iki algoritma gibi Feistel yapısını kullanır. IRON, 64 bitlik veri bloklarını 128 bitlik anahtarla şifrelemede kullanılır. Döngü (round) sayısı 16 ile 32 arasındadır. Alt anahtarlar döngü sayısına bağlıdır. Alt anahtarların sayısı döngü sayısına eşittir. Bu nedenden dolayı algoritma anahtar bağımlıdır. IRON algoritmasının var olan algoritmalardan farkı da budur. Bu algoritmanın avantajı bitler yerine 16-tabanındaki sayılar kullanmasıdır, dezavantajı ise yazılım için tasarlanmış olmasıdır.

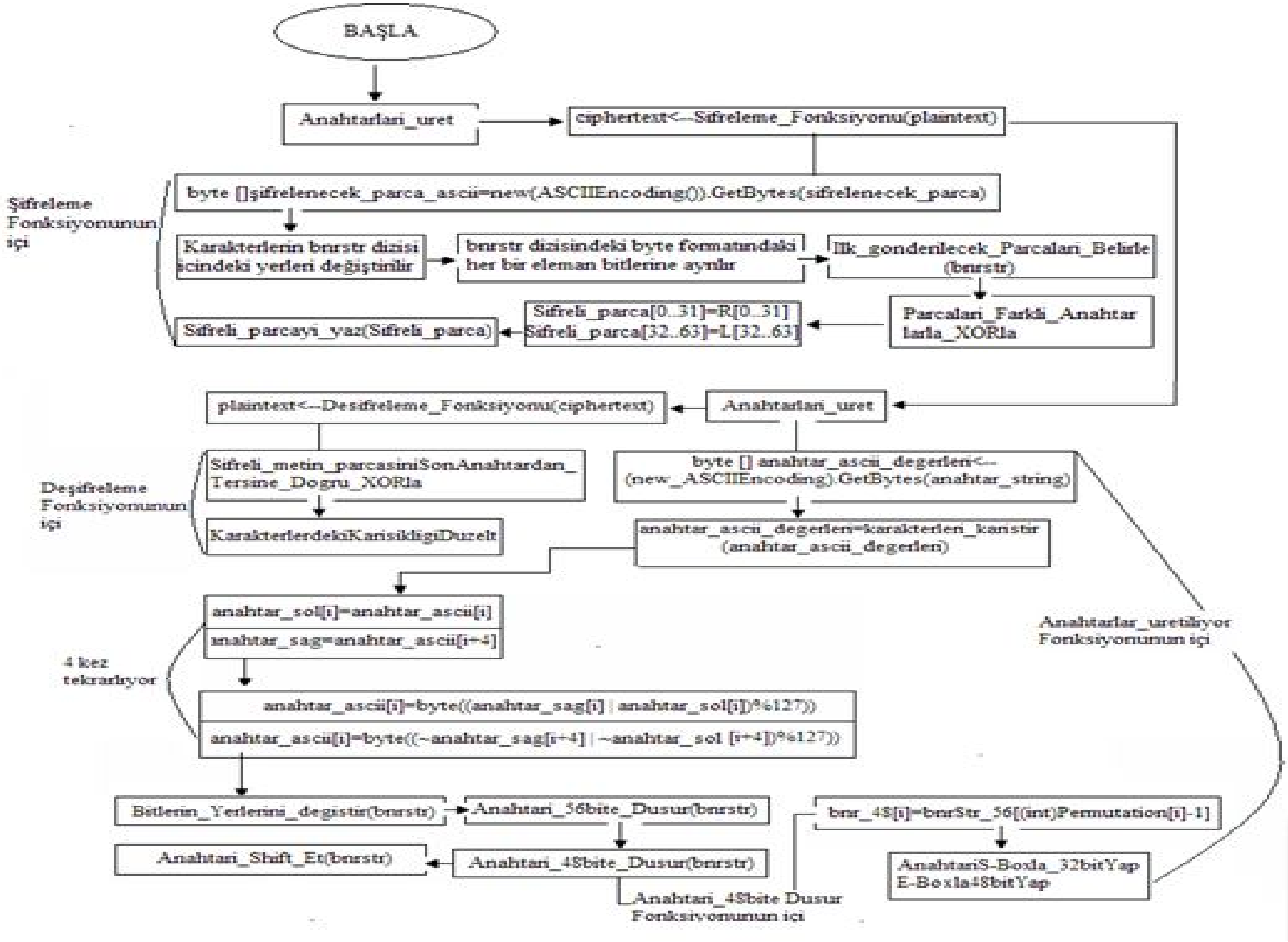
- **4-AES (The Advanced Encryption Standard) :** AES, John Daemen ve Vincent Rijmen tarafından Rijndael adıyla geliştirilmiş ve 2002 yılında standart haline gelmiştir. AES uzunluğu 128 bitte sabit olan blok ile uzunluğu 128, 192 ya da 256 bit olan anahtar kullanır. Kullanılan tekniklerden bazıları baytların yer değiştirmesi, 4x4' lük matrisler üzerine yayılmış metin parçalarının satırlarına uygulanan kaydırma işlemleridir. 2006 yılı itibariyle en popüler simetrik algoritmalardan biridir.

Algoritmanın Detayları

Şifreleme Algoritması

- Şekil 2'de belirtilen şifreleme algoritmasında kullanıcıdan şifrelenmesi istenen bir düz metin ve anahtar girmesi beklenmektedir. Anahtar uzunluğu sabit olmakla beraber 64 bittir. Yani 8 karakter uzunluğuna denk gelmektedir. Anahtar herhangi bir sayı, alfabede yer alan harfler ya da özel karakterler olabilir. Türkçe karakterler içerisinde bulunan ş,ğ,ö,ç,ü gibi harfler girildiğinde ise bu karakterler s,g,o,c,u harfleriyle yer değiştiriliyor. Temel şifreleme işlemi Şekil 2'de belirtilmiştir. Kullanılan yapı Feistel'dir.
- Anahtar uzunluğu 64 bitten kısa girildiğinde kullanıcıya 64 bitten daha kısa uzunlukta anahtar girmemesini söyleyen bir hata mesajı gönderiliyor. Eğer anahtar uzunluğu 64 bitten büyük girilirse ilk 64 biti alınıp geri kalan kısmı önemsenmiyor.

- Alt anahtarlar 64 bitlik anahtar kullanılarak üretiliyor. Alt anahtarların sayısı 16 ve her biri 48 bitten oluşmakta. Anahtar boyutları DES algoritmasıyla aynı ancak alt anahtarları üretmede kullanılan işlemler farklı.
- Şifrelenecek metnin uzunluğu kullanıcının isteğiyle değişiklik gösteriyor. Sadece bir karakter olabileceği gibi çok uzun bir metin de olabilir. Ancak şifreleme algoritmasında bloklar halinde şifreleme tekniği kullanıldığından metin 64 bitlik bloklara bölünüyor.



Şekil2.Algoritmanın Şematik gösterimi

Deşifreleme Algoritması

- çözmek için öncelikle şifreli metnin ilk 64 bitlik bloğundan başlanır. Bu bloğun şifresi çözüldükten sonra eğer varsa diğer 64 bitlik blok deşifre edilir. Bu işlem şifreli metnin sonuna kadar devam eder.
- Şifreyi çözmede kullanılan fonksiyonda şifreli metin bloğu bitlerine ayrılır. Bu bitlerden ilk 32 si L0 parçasını, geri kalan 32 bit ise R0 parçasını

ÖRNEK UYGULAMA

- Düz Metin: *Kriptoloji şifreleme ve deşifreleme işlemlerini kapsayan bir bilimdir ve diğer bilimlerde olduğu gibi bu biliminde bir tarihi vardır.*
- Anahtar*: Simetrik şifreleme bir mesajın gizliliğini sağlamak için kullanılan bir şifreleme türüdür.*
- Şifrelenmiş-Metin: *25F221670F1FEC9C5DD9DD1B0E16EF0389DB391A524AF1C9D019568830E98A6C7B1C069A62BE11AD810A01AEC139168AC82AA81F468A1108DD22099E8650E7DB5C5CDADACF96FC46F9131DC7D518268ED21F008536E5CB76D91AA31AE6BE3728F1472C82DD582682DB484A5E09C4BF85DD0213B014506FD52CDA8CBF33CAB039940955DA74EDD57B*
- De-şifre Edilmiş Metin: *Kriptoloji sifreleme ve de-sifreleme islemlerini kapsayan bir bilimdir ve diger bilimlerde oldugu gibi bu biliminde bir tarihi vardir.* (ASCII kodlamadaki kısıtlamalardan dolayı düz metin *hexadecimal* formda gösterilmiştir).

RC4 Şifreleme Algoritması

- RC4 Şifreleme Algoritması
  RC4, bir anahtar ile bir metni şifrelemeye yarayan bir şifreleme algoritmasıdır, yaygın olarak kullanılır ve genelde mesajları şifrelemede kullanılır.

HAZIRLAYAN

Yunus Emre Kolay
T12-D / 2225