**AES (Advanced Encryption Standard) Şifreleme Yöntemi**

**1. AES Nedir?**

AES, simetrik anahtar şifreleme algoritmasıdır ve dünya genelinde verilerin güvenli bir şekilde şifrelenmesi için yaygın olarak kullanılmaktadır. AES, 2001 yılında ABD Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) tarafından **rijndael** algoritması olarak seçilmiştir ve 128, 192, ve 256 bit anahtar uzunluklarıyla çalışabilir.

AES, verileri bloklar halinde işler. AES, şifreleme ve şifre çözme işlemleri için aynı anahtarı kullanır, bu da onu **simetrik şifreleme algoritması** yapar.

**2. AES'in Temel Özellikleri**

* **Blok Boyutu**: AES, 128-bitlik veri blokları kullanarak veriyi işler. Yani her şifreleme veya şifre çözme işleminde, veriler 128 bitlik bloklar halinde ele alınır.
* **Anahtar Uzunluğu**: AES, üç farklı anahtar uzunluğu kullanır:
  + **AES-128**: 128 bitlik anahtar (16 byte)
  + **AES-192**: 192 bitlik anahtar (24 byte)
  + **AES-256**: 256 bitlik anahtar (32 byte)
* **Şifreleme ve Şifre Çözme**: AES, şifreleme işlemi için bir **gizli anahtar** (secret key) kullanır. Bu anahtar, veriyi şifrelerken ve şifre çözerken aynı olur.

**3. AES Şifreleme Adımları**

AES, her işlemde belirli bir dizi adımdan geçer. Bu adımlar şunlardır:

1. **Anahtar Genişletme (Key Expansion)**: AES, verilen anahtarı kullanarak daha küçük anahtarları genişletir ve bu genişletilmiş anahtarlar, her "round" (tur) için kullanılır. Anahtar genişletme, AES'in şifreleme işlemi için gerekli olan alt anahtarları üretir.
2. **Başlangıç Durumu (Initial Round)**:
   * **Add Round Key**: İlk olarak, veri bloğu (plaintext) ile genişletilmiş anahtarlardan birisi XOR işlemi ile birleştirilir.
3. **Ana Döngü (Main Rounds)**: AES-128 için bu döngü 9 kez tekrarlanır, AES-192 için 11, AES-256 için ise 13 kez tekrarlanır. Her turda şu işlemler yapılır:
   * **SubBytes**: Bu adımda her byte, sabit bir S-Box (substitution box) kullanılarak yer değiştirir.
   * **ShiftRows**: Bu adımda veri matrisindeki her satır kaydırılır.
   * **MixColumns**: Bu adımda, her sütun bir matematiksel işlemle karıştırılır.
   * **Add Round Key**: Bu adımda, genişletilmiş anahtarların bir kısmı ile veri blokları XOR işlemine tabi tutulur.
4. **Son Dönüşüm (Final Round)**: Ana döngüden sonra son bir "round" (tur) yapılır. Bu final round'da **MixColumns** işlemi yapılmaz.
5. **Şifreli Metnin Oluşması**: Şifreleme işlemi tamamlandığında, şifreli metin (ciphertext) elde edilir.

**4. AES Modları**

AES, farklı şifreleme modlarıyla çalışabilir. Bu modlar, AES'in nasıl çalışacağını belirler. Yaygın olarak kullanılan modlar şunlardır:

* **ECB (Electronic Codebook) Modu**: En basit şifreleme modudur. Her blok bağımsız bir şekilde şifrelenir. Ancak, aynı plaintext blokları her zaman aynı ciphertext'e dönüştüğü için güvenlik riski yaratabilir.
* **CBC (Cipher Block Chaining) Modu**: Verilen her blok, önceki blokla XOR işlemi yapılır. Bu, daha güvenli bir şifreleme sağlar çünkü aynı plaintext blokları her seferinde farklı ciphertext'lere dönüştürülür.
* **CFB (Cipher Feedback) ve OFB (Output Feedback) Modları**: Bu modlar, blok şifreleme algoritmasını akış şifrelemesi gibi çalıştırarak daha esnek şifreleme sağlar.
* **CTR (Counter) Modu**: Her blok için benzersiz bir sayaç değeri oluşturulup XOR işlemiyle şifreleme yapılır. Bu mod paralel şifreleme yapabilme avantajı sağlar.

**5. AES'in Güvenliği**

AES, güvenliği konusunda oldukça güçlüdür. Anahtar uzunluğunun 128, 192 veya 256 bit olması, potansiyel bir saldırıyı zorlaştırır. AES, **brute force** (kaba kuvvet) saldırılarından etkilenmeyecek kadar güçlüdür ve bu nedenle birçok ulusal güvenlik kurumları ve özel şirketler tarafından kullanılır.

* AES-128, günümüzde çoğu uygulama için yeterince güvenli kabul edilmektedir. Ancak, bazı güvenlik uzmanları uzun vadeli güvenlik için AES-256'nın tercih edilmesini önerir.
* AES, **differential cryptanalysis** ve **linear cryptanalysis** gibi bilinen modern şifre kırma tekniklerine karşı oldukça dayanıklıdır.

**6. AES Uygulama Alanları**

AES, çeşitli alanlarda kullanılır, bunlar arasında:

* **VPN (Virtual Private Network)** şifrelemesi
* **Wi-Fi güvenliği** (WPA2)
* **Veri şifreleme** (dosya şifreleme, disk şifreleme)
* **SSL/TLS** protokollerinde güvenli iletişim için kullanılır
* **Kripto para birimleri** gibi dijital ödeme sistemlerinde

**7. AES İle Şifreleme ve Şifre Çözme Örneği**

AES ile şifreleme işlemi aşağıdaki adımları içerir:

1. Bir anahtar (örneğin, 128 bit) ve şifrelenecek veri (plaintext) belirlenir.
2. Anahtar ve veri, AES algoritmasına girer.
3. AES, anahtarı ve veriyi işlemeye başlar, bloklar halinde şifreler.
4. Sonuç olarak, ciphertext (şifreli veri) elde edilir.

Şifre çözme işlemi de aynıdır, ancak şifreli veriye (ciphertext) aynı anahtar ile işlemler yapılır.

**Soru:**

Bir veriyi AES-128 şifreleme algoritması ile şifrelemek istiyorsunuz. Şifrelenecek mesaj **"Hello World!"** ve şifreleme için kullanılacak anahtar **"Th1s1sA128BitKey!"**.

1. Verilen **şifreli mesajı (ciphertext)** elde edin.
2. Şifreyi çözmek için doğru **özel anahtar** ile AES-128 şifre çözme işlemini yaparak **orijinal metni (plaintext)** geri elde edin.

**Çözüm Adımları:**

**Adım 1: Verilen Bilgiler**

* **Anahtar (key)**: "Th1s1sA128BitKey!" (128-bit anahtar, yani 16 byte)
* **Şifrelenecek mesaj (plaintext)**: "Hello World!"

**Adım 2: AES-128 Şifreleme**

AES-128 şifreleme algoritması, 128 bitlik bir anahtar kullanarak veriyi şifreler. Bu işlemde, veriler bloklar halinde işlenir ve her blok AES'in şifreleme adımlarından geçer.

1. **Anahtar Genişletme**: 128 bitlik anahtar, şifreleme işlemine başlamak için kullanılır. AES şifrelemesi her "round" (tur) için ayrı anahtarlar gerektirir. Bu, anahtar genişletme süreci ile yapılır.
2. **Şifreleme İşi**:
   * AES şifrelemesi dört temel adımdan oluşur: **SubBytes**, **ShiftRows**, **MixColumns**, ve **AddRoundKey**.
   * Bu adımların amacı, mesajın her bitini karmaşık bir şekilde değiştirmektir. Sonuçta, her adımda verinin yapısı ve içeriği daha güvenli hale gelir.
3. **Mod Seçimi (Şifreleme Modu)**:
   * AES şifreleme için çeşitli modlar mevcuttur. Bu soruda **CBC (Cipher Block Chaining)** modunu kullanıyoruz. Bu modda her veri bloğu, önceki bloğun şifreli çıktısı ile XOR yapılır, böylece aynı veriler her seferinde farklı şifreli verilere dönüşür. Bu, şifrelemenin güvenliğini artırır.
4. **Şifreli Mesaj (Ciphertext)**:
   * Verilen mesaj, anahtar ve şifreleme moduna göre şifrelenir. **CBC modu** ve **128 bitlik anahtar** kullanıldığında, her seferinde şifreli mesaj (ciphertext) değişecektir çünkü kullanılan **Initialization Vector (IV)** rastgele seçilir.

**Adım 3: Şifreyi Çözme**

AES, **simetrik bir şifreleme algoritmasıdır**, yani şifreleme ve şifre çözme işlemleri için aynı anahtar kullanılır. Bu nedenle, şifreyi çözmek için verilen anahtarı kullanacağız.

1. **AES-128 Şifre Çözme**:
   * AES-128 ile şifre çözme işlemi, şifreleme adımlarının tersine yapılır. Bu adımlar şunlardır:
     + **AddRoundKey**: Şifreli veriye son anahtar eklenir.
     + **InverseShiftRows**: Satır kaydırma işlemi tersine yapılır.
     + **InverseSubBytes**: SubBytes adımının tersine, her byte yeniden değiştirilir.
     + **InverseMixColumns**: MixColumns adımının tersi yapılır.
     + **Final AddRoundKey**: Son anahtar ile XOR işlemi yapılır.
2. **Orijinal Mesaj (Plaintext)**:
   * Şifreli mesaj ve doğru anahtar kullanılarak şifre çözme işlemi tamamlanır ve orijinal mesaj olan **"Hello World!"** geri elde edilir.

**Sonuç:**

AES-128 ile şifreleme ve şifre çözme işlemlerinde, aynı anahtar kullanılarak veri güvenli bir şekilde şifrelenir ve tekrar çözülür. Verilen örnekte:

* Şifreli mesaj, doğru anahtar ve IV ile çözüldüğünde orijinal metin **"Hello World!"** olarak elde edilir.

**Özet:**

* **Şifreleme**: AES-128 algoritması ile, belirlenen anahtar ve mod ile veri şifrelenir.
* **Şifre Çözme**: Aynı anahtar ile şifre çözme işlemi yapılır ve orijinal veri (plaintext) geri elde edilir.
* AES, simetrik bir şifreleme algoritması olduğu için şifreleme ve şifre çözme işlemleri için aynı anahtar kullanılır.