Kriptografik Algoritmaların Karşılaştırılması

Proje Ekibi: Rüştü Koray Özkök, Furkan Ulutaş

Danışman: Dr. Öğr. Üyesi Resmiye Nasiboğlu

Amaç

Bu projede kriptografik algoritmaların birbirleri arasındaki farklarını uygulamalar ile örneklendirerek doğrulayıp, avantajlarını, dezavantajlarını tartarak yorumlayıp ortak bir sonuca varmak istiyoruz.

Hedef

Hedefimiz AES(Advanced Encryption Standard) algoritmasını ChaCha20-Poly1305 ismi ile bilinen bir AEAD(Authenticated Encryption with Additional Data) algoritması,DES(Data Encryption Standard),3DES(TripleDES) ve RSA(Rivest-Shamir-Adleman) şifreleme algoritmalarıyla karşılaştırıp sonuçların analiz edilmesinden oluşacaktır.

Analiz

Karşılastırmalar da dikkate alınması gereken önemli hususlar şöyle belirlenmiştir:

- Hafıza(Memory)
- Uygulama Süresi(Execution time)
- Güvenlik (Security)
- Karışıklık (Complexity)

Algoritma Uygulamaları

- **AES ile şifreleme ve şifre çözme ekran çıktısı**

```
Enter message to encrypt: hello
Enter encryption key: 12345
After padding: hello

Encrypted Message: b'r3V0A0Ssjw/4ZOKL42/hWSQOLKy7lt9bOVt7D75RA3E='
Decrypted Message: hello
```

- **DES ile şifreleme ekran çıktısı**

```
D:\Scripts\UEM>py -2.7 encrypt_foo.py
('The plain text is : ', 'I see you')
('The encoded string is : ', 'UH562EGM8RCHHTOUC5CTRS59OG======')

D:\Scripts\UEM>
```

- **DES ile şifre çözme çıktısı**

```
D:\Scripts\UEM>py -2.7 e.py
The ecrypted string is : UH562EGM8RCHHTOUC5CTRS59OG======
The plain text is : I see you

D:\Scripts\UEM>
```

- **ChaCha20 Uygulaması**

{"nonce": "IZScZh28fDo=", "ciphertext": "ZatgU1f30WDHriaN8ts="}

Algoritma Uygulamaları

- **RSA ile şifreleme ekran çıktısı**


```
Public key:
(n=0x9a11485bccb9569410a848fb1afdf2a81b17c1fa9f9eb546fd1deb873b49b693a4edf20e36
ffc3da9953657ef8bee80c49c2c12933c8a34804a00eb4c81248e01f, e=0x10001)
 -----BEGIN PUBLIC KEY-----
 MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCaEUhbzL1WlBCoSPsa/fKoGxfB
 +p+etUb9HeuHO0m2k
 -----END PUBLIC KEY-----
 Private key:
(n=0x9a11485bccb9569410a848fb1afdf2a81b17c1fa9f9eb546fd1deb873b49b693a4edf20eb8
362c085cd5b28ba109dbad2bd257a013f57f745402e245b0cc2d553c7b2b8dbba57ebda7f84cfb3
2b7d9c254f03dbd0188e4b8e40c47b64c1bd2572834b936ffc3da9953657ef8bee80c49c2c12933
c8a34804a00eb4c81248e01f,
d=0x318ab12be3cf0d4a1b7921cead454fcc42ba0704626394833394d6fb9529547827e9c8d23517
b5566dd3d3e5b16ec737987337a0e497fdba4b5ad97af41c1c3cdd87542a4637d81)

 -----BEGIN RSA PRIVATE KEY-----

 MIICXAIBAAKBgQCaEUhbzL1WlBCoSPsa/fKoGxfB+p+etUb9HeuHO0m2k6Tt8g64
 N1wIXNWy16EJ260r0legE/V/dFQC4kWwzC1VPHsrjbu1fr2n+Ez7MrfZw1TwPb0B
 iOS45AxHtkwb01coNLk2/BPamVNlfv1+6Ax3wsEpM81j5ASgDrTIEkjgHwIDAQAB
 AoGAMYqxK+PPDUobeSHOrUVPzEK6BwRiY5SDOU1vuVKVR4J+nI0jspSo4B+KEBna
 NONQ8jB3QOBqJwvvH+ZG5q0hPjG1KP3V9dA+YzwHxEdV7WIqYp156CLAlevfnMgO
 UXtVZt09P1sW7HN5hzN6Dk1/26S1rZevQcHDzdh1QqRjfYECQQDGDUIQX1OiAcGo
 d5YqAGpNe0wz J0UypeqZcqS9MVe9OkjjopCkkYnt1fdN/1oG7S/1KUMtLoGHqntb
 c428zOO/AkEAxyV0cmuJbFdfM0x2XhZ+ge/7putIx76RHDOjBpM6VQXpLEFj54kB
 qGLAB7SXr7P4AFrEjfckJOp2YMI5BrebоQJAb3EUZHt/WeDdJLutzpKPQ3x7oykM
 wfQkbxXYZvD16u96BkT6WO/gCb6hXs05zj32x1/hgfHyRvGCGjKKZdtwpwJBAJ74
 y0g7h+wwox J0S1k4Y6yeQ1kxUVwCSBxXLCCnjr0ohsaJPJMrz2L30YtVInFkHO1L
 i/Q4AWZmtDDxWkx+bYECQG8e6bGoszuX5xjvhEBs1Ivs9+nMzMuYBR8HvhLo58B5
 N8dk3nIsLs3UncKLi1WubMAc1U5jUxZoqWpRXXwECKE=

 -----END RSA PRIVATE KEY-----

 Encrypted:
b'99b331c4e1c8f3fa227aacd57c85f38b7b7461574701b427758ee4f94b1e07d791ab70b55d672
ff55dbe133ac0bea16fc23ea84636365f605a9b645e0861ee11d68a7550be8eb35e85a4bde6d73b
0b956d000866425511c7920cdc8a3786a4f1cb1986a875373975e158d74e11ad751594de593a35d
e765fe329c0d3dfbbfedc'
```


Karşılaştırmalar

- **AES ve DES**

AES, matematiksel olarak daha verimli ve zarif bir şifreleme algoritmasıdır, ancak asıl gücü anahtar uzunluğu seçeneklerinde yatmaktadır. AES'e kıyasla DES'te şifreleme de çok daha hızlıdır.

- **AES ve 3DES**

Her şey sabit tutulduğunda, AES, 3DES'e kıyasla çok daha hızlıdır. Güvenlik söz konusu olduğunda da, pratik kullanımda hala kırılmaz olarak kabul edildiğinden AES kazanandır.

- **AES ve RSA**

Simetrik anahtarlar ve asimetrik anahtarlar farklı amaçlar için kullanılmaktadır. Simetrik olan AES, hesaplama açısından daha basittir ve büyük miktardaki veriyi hareketsiz halde şifrelemek için kullanılır. RSA önemli miktarda hesaplama gerektirir, bu nedenle küçük miktarlardaki veriler için kullanılır.

- **AES ve ChaCha20**

ChaCha20, sadeliği nedeniyle neredeyse kesinlikle yeni tasarımlar için daha iyi bir seçimdir. ChaCha20'ye veya türevlerine saldırmak, AES'e saldırmaktan daha zordur ve performansı daha fazladır.

Sonuç ve Değerlendirme

AES algoritması, her 128 bitlik veri bloğuna art arda bir dizi matematiksel dönüşüm uygular. Bu yaklaşımın hesaplama gereksinimleri düşük olduğundan, AES, dizüstü bilgisayarlar ve akıllı telefonlar gibi tüketici bilgi işlem cihazlarıyla ve büyük miktarda veriyi hızla şifrelemek için kullanılır.

RSA şifrelemesi genellikle diğer şifreleme şemalarıyla birlikte veya bir mesajın gerçekliğini ve bütünlüğünü kanıtlayabilen dijital imzalar için tercih edilir. Simetrik anahtarlı şifrelemeden daha az verimli ve kaynak ağırlıklı olduğundan, genellikle tüm iletileri veya dosyaları şifrelemek için kullanılmaz.

Data Encryption Standard olan DES artık güvenli olarak kabul edilemez. İç kısımlarında büyük kusurlar bilinmemekle birlikte, 56 bitlik anahtarı çok kısa olduğu için temelde yetersizdir.

ChaCha20 ve türevlerinin hızı ve basitliği ve de sorunsuz çalışması için herhangi bir donanıma ihtiyaç duymaması, zaman geçtikçe, genellikle veri yönetimi ile ilgilenen şirketlerin AES yerine ChaCha20 şifrelemesini seçmesine neden oluyor.

Kaynakça

- Gupta A. & Waila K. (2014). Cryptography Algorithms: A Review. Fatehgarh Sahib,India: Sri Guru Granth Sahib World University.
- Chandra S. & fri.(2014). A Comparative Survey of Symmetric and Asymmetric Key Cryptography. India,Kolkata: 2014 International Conference on Electronics, Communication and Computational Engineering(ICECCE).
- Mushtaq Faheem M. & fri.(2017). A Survey on the Cryptographic Encryption Algorithms. Malaysia,Johor,Batu Pahat,Parit Raha: Universiti Tun Hussein Onn Malaysia(UTHM). International Journal of Advanced Computer Science and Applications,Vol. 8, No.11, 2017(IJACSA).
- Daemen J. & Rijmen V.(1999). AES Proposal: Rijndael.Belgium,Brussel:Katholieke Universiteit Lueven,ESAT-COSIC.
- WEB_1.(2018).Nir Y & Langley A. Internet Research Taskforce (IRTF) document on ChaCha20 and Poly1305 for IETF protocols.
- WEB_2. Python package and info.