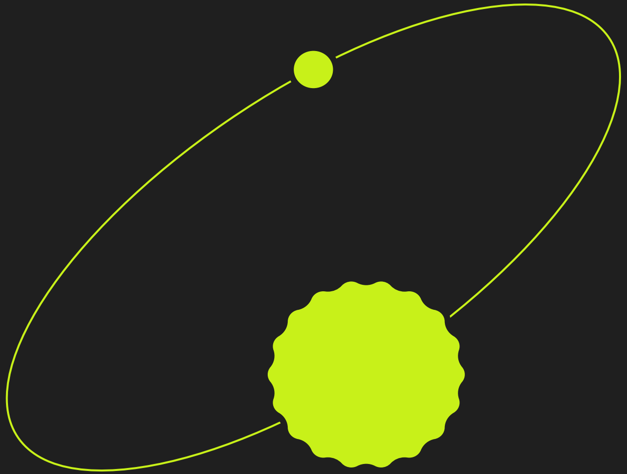
Introduction to Cryptography



Workshop By Fodhil Benhiba

Table of contents

01

What is Cryptography?

02

Types of Cryptography

03

Hands on practice

04

Applications of Cryptography

05

Q&A

06

Ressources

01

What is Cryptography?

Cryptography is the practice of securing communication against potential threats. More generally, cryptography is about constructing and analyzing protocols that prevent third parties or the public from reading private messages.

02

Types of cryptography

Types of Cryptography

1. Symmetric Cryptography

2. Asymmetric Cryptography

3. Hash functions

Symmetric Cryptography

Symmetric cryptography, employs a single shared secret key for both encryption and decryption of data.

Steam Cipher

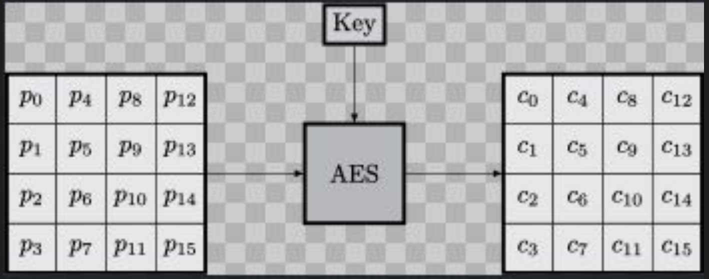
Block Cipher

AES

(Advanced Encryption Standard)

AES encrypts a block of 16 bytes only at a time,using an operating mode, the most used modes are: ECB, CBC, CTR, OFB, CFB, GCM. Basically, there are four operations on the state matrix, each important for the security of AES:

- add round key
- shift row
- substitution box
- mix column



p_0	p_4	p_8	p_{12}
p_1	p_5	p_9	p_{13}
p_2	p_6	p_{10}	p_{14}
p_3	p_7	p_{11}	p_{15}

c_0	c_4	c_8	c_{12}
c_1	c_5	c_9	c_{13}
c_2	c_6	c_{10}	c_{14}
c_3	c_7	c_{11}	c_{15}

Asymmetric Cryptography

Asymmetric cryptography, also known as public-key cryptography, utilizes pairs of mathematically related keys: a public key and a private key.This approach enables secure communication and authentication without the need for prior key exchange.

RSA

(Rivest-Shamir-Adleman)

1-Choose two large prime numbers p and q.

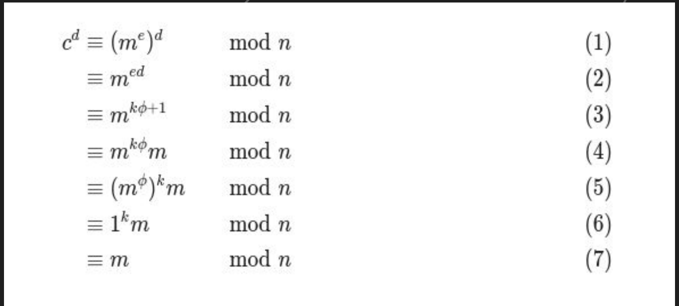
2-Compute n = pq.

3-Compute λ(n), where λ is Carmichael's totient function.

4-Choose an integer e such that 1 < e < λ(n) and gcd(e, λ(n)) = 1; that is, e and λ(n) are coprime.

5-Determine d as d ≡ e**−1 (mod λ(n));

```
 - Encryption:
     c = m ** e % n
 - Decryption
     m = c ** d % n
```



$$\begin{aligned}
c^d &\equiv (m^e)^d && \bmod n && (1)\\
&\equiv m^{ed} && \bmod n && (2)\\
&\equiv m^{k\phi+1} && \bmod n && (3)\\
&\equiv m^{k\phi}m && \bmod n && (4)\\
&\equiv (m^{\phi})^k m && \bmod n && (5)\\
&\equiv 1^k m && \bmod n && (6)\\
&\equiv m && \bmod n && (7)
\end{aligned}$$

Hash Functions

A hash function is a function that takes an arbitrary length input and produces a fixed length output. They are used to securely store passwords, verify data integrity. Common hash functions include Bcrypt, SHA-256, MD5.

03

Hands on practice

04

Applications of Cryptography

Cryptographic Protocols

Cryptographic protocols are sets of rules and procedures implemented in communication systems to ensure secure data transmission

TLS

(Transport Layer Security)

TLS is commonly used to secure web traffic (HTTPS).
Once the client and server have agreed to use TLS, they negotiate a stateful connection by using a handshaking procedure.

How TLS handshake is done?

1- Client Hello (TLS version, Cipher suits)

2- Server Hello (certificate, public key)

3- Client verifies TLS Certificate

4- The client creates secret key that's encrypted using the public key.

5- Server decrypts the secret key with its own private key.

6- Client and server completed a process to generate a secret key that can now be used for encryption and decryption.

05

Q&A

06

Ressources

Ressources

https://cryptohack.org/

https://www.hackthebox.com/

https://picoctf.org/

References

https://www.avast.com/c-what-is-transport-layer-security

https://wikipedia.org/

https://cryptohack.gitbook.io/

https://www.internetsociety.org/deploy360/tls/basics/

Thank You!