CYBER CHALLENGE
CyberChallenge.IT

cini
Cybersecurity National Lab

SPONSOR PLATINUM

SPONSOR GOLD

SPONSOR SILVER

Perfect secrecy, cryptoanalysis and attack models

Rocco DE NICOLA

IMT Lucca

CYBER CHALLENGE
CyberChallenge.IT

cini Cybersecurity National Lab

https://cybersecnatlab.it

License & Disclaimer

License Information

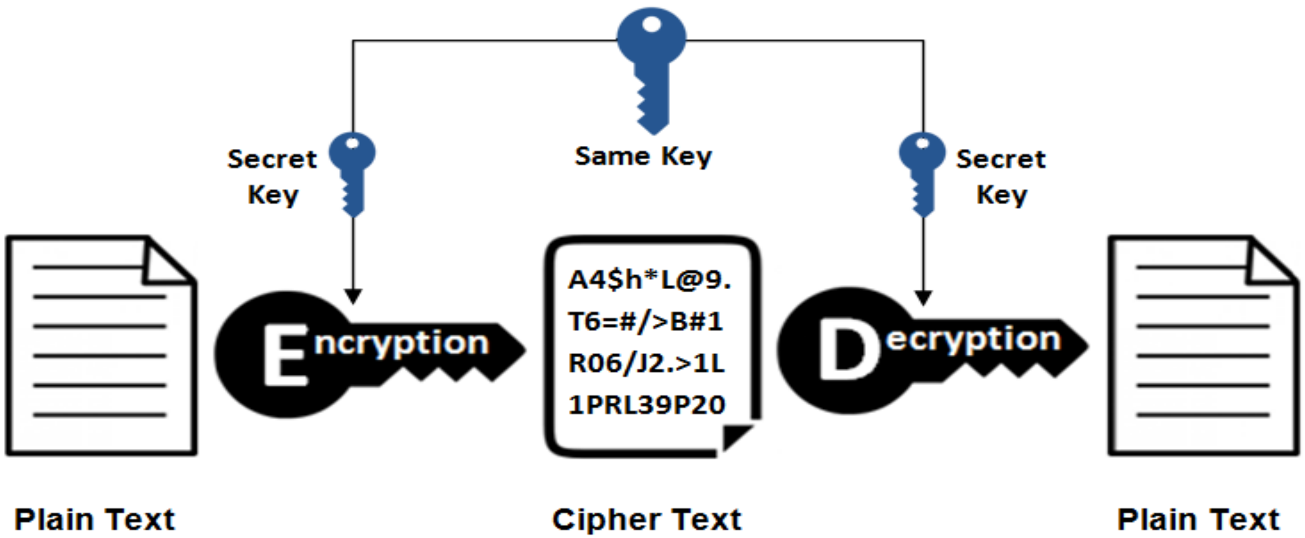
Disclaimer

Outline

- Cryptoanalysis
- Attacker’s model
- Attack techniques
- Perfect encryption

Symmetric key cryptography

- Requires that both sender and recipient know the same key.
- An issue is how they do share it without meeting.



Crypto analysis

- Cryptanalysis is a set of techniques, set up
  - to test the robustness of the algorithm and of the key by trying possible attacks against it
  - to break the code and infer the key from the available ciphertext or decrypt the ciphertext without knowing key
- Two kinds of attacks:
  - Analytic
  - Brute-force

Safe encryption

- A symmetrical encryption pattern is safe if:
  - The sender and the receiver receive and keep the key safely (no attacker must intercept the key).
  - The encryption algorithm is robust, i.e., an attacker in possession of a certain number of ciphertexts, but not of the encryption key, is unable to infer the plaintext or the key
- It is assumed that the algorithm is known and that it is impractical to decipher messages by having only ciphertexts (Kerckhoffs's principle).

Kerckhoffs's principle

- *The encryption scheme* is not secret
  - The attacker knows the encryption scheme
  - The only secret is the *key*
  - The key must be chosen at random and kept secret
- Some arguments in favor of this principle:
  - Easier to keep *key* secret than *algorithm*
  - Easier to change *key* than to change *algorithm*
  - Simplifies standardization:
    - Ease of deployment
    - Public validation

Crypto analysis application

- Cryptanalysis techniques can be applied starting from different "hypotheses" about the information possessed by the attacker:
  - Not knowing anything, not even the algorithm
  - Knowing some ciphertexts and the algorithm
  - Knowing also some plaintexts.

Attacker’s Knowledge

- *Ciphertext only*: A collection of ciphertexts
- *Known plaintext*: A collection of ciphertexts and one or more pairs <plaintext, ciphertext>
- *Chosen plaintext*: A collection of <plaintext, ciphertext> pairs with plaintexts selected by the attacker
- *Chosen ciphertext*: A collection of <plaintext, ciphertext> pairs with ciphertexts selected by the attacker
- *Chosen text*: Two collections of pairs, <plaintext, ciphertext> one with chosen text and the other with chosen ciphertext

Cryptonalitic Attacks

- The attacker tries:
  - to deduce the key used from a specific plain text, to compromise all future and past messages encrypted with that key
  - to guess the plain text from the encrypted text
- The attacker leverages on:
  - the knowledge of the encryption algorithm
  - some knowledge of the general characteristics of plaintext
  - (possibly) some sample pairs of <plaintext, ciphertext>.

Brute force attacks

- The attacker:
  - Tries all possible keys on some ciphertexts until an intelligible translation into plaintext is obtained.
  - On average, half of all possible keys must be tried to achieve success.
- The attacker must have:
  - Some degree of knowledge of the expected plaintext.
  - Some means to automatically distinguish plain texts from ciphered texts.

Time required for exhaustive key trials

Key Size (bits)	Number of Alternative Keys	Time Required at 1 Decryption/μs	Time Required at 10^6 Decryptions/μs
32	$2^{32} = 4.3 \times 10^9$	$2^{31} \mu s = 35.8$ minutes	2.15 milliseconds
56	$2^{56} = 7.2 \times 10^{16}$	$2^{55} \mu s = 1142$ years	10.01 hours
128	$2^{128} = 3.4 \times 10^{38}$	$2^{127} \mu s = 5.4 \times 10^{24}$ years	5.4×10^{18} years
168	$2^{168} = 3.7 \times 10^{50}$	$2^{167} \mu s = 5.9 \times 10^{36}$ years	5.9×10^{30} years
26 characters (permutation)	$26! = 4 \times 10^{26}$	$2 \times 10^{26} \mu s = 6.4 \times 10^{12}$ years	6.4×10^6 years

If checking one key takes 1000 clock cycles, a 1 Gigahertz computer (with 1,000,000,000 cycles per second) will check 1 million keys per second and needs 1 microsec per key

Levels of security

- Unconditional security: no matter how much computer power or time is available, the cipher cannot be broken since the ciphertext provides insufficient information to uniquely determine the corresponding plaintext
- Computational security: given limited computing resources (e.g., the time needed for calculations is greater than age of universe), the cipher cannot be broken
- Quantum Computers might change the scene: it might be possible to create specific algorithms for them that dramatically reduce the time needed to break cryptographic algorithms.

Confusion and Diffusion

- Cipher needs to completely obscure statistical properties of original message
- Shannon suggested combining elements to obtain:
  - *diffusion* – dissipates statistical structure of plaintext over bulk of ciphertext
  - *confusion* – makes relationship between ciphertext and key as complex as possible
- Avalanche effect: When an input is changed slightly, the output has to change significantly: very small changes to the plaintext or the key lead to a big changes in the ciphertext

Perfect secrecy

- Perfect secrecy is based on the idea that for any two messages m1, m2 and any ciphertext c, the probability of obtaining c as the result of the encryption of m1 or m2 is the same.
- Symmetric encryption algorithms rely on substitutions and transpositions. Even for the best of those currently in use, it is not known whether there can be an efficient cryptanalytic procedure that can reverse these transformations without knowing the encryption key.
- Asymmetric encryption algorithms depend on mathematical problems that are thought to be difficult to solve. There is no proof that these problems are hard, and a mathematical breakthrough could make systems vulnerable to attack.

Perfect encryption with OTP

- One-time pad (OTP) is an encryption technique that cannot be cracked, but requires a pre-shared key at least the same size as the message
- A plaintext is paired with a random secret key (the one-time pad).
- Each bit or character of the plaintext is encrypted by combining it with the corresponding one from the pad using modular addition (XOR).
- If the key is truly random and never reused (in whole or in part), the resulting ciphertext will be impossible to decrypt.
- Any cipher scheme, to guarantee perfect secrecy, must use keys with effectively the same requirements as OTP keys (slightly impractical!)

Grazie

CYBER CHALLENGE
CyberChallenge.IT

cini
Cybersecurity National Lab

SPONSOR PLATINUM

SPONSOR GOLD

SPONSOR SILVER