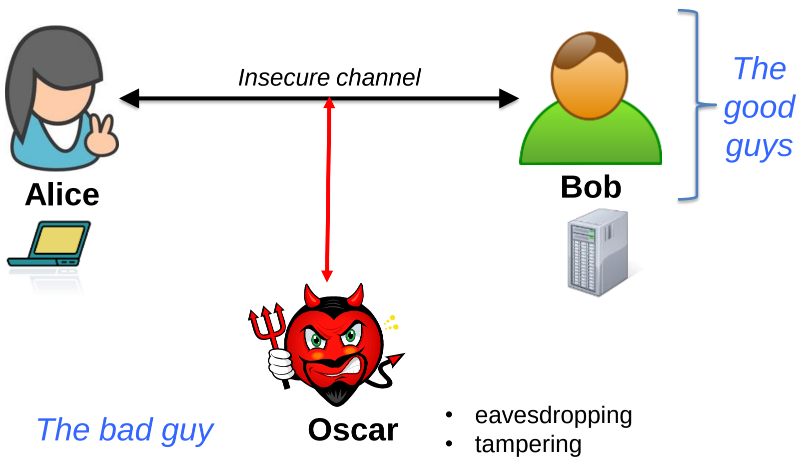
Symmetric Encryption

Gianluca Dini
Dept. of Ingegneria dell’Informazione
University of Pisa
gianluca.dini@unipi.it

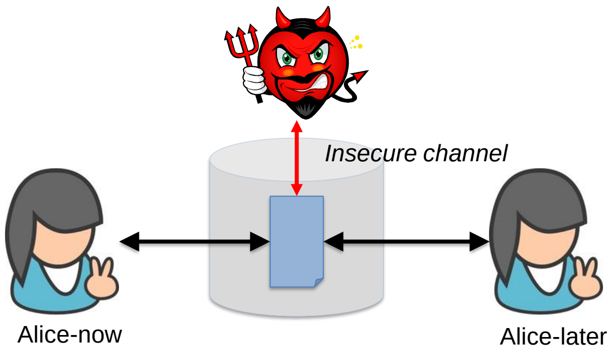
1

Main characters



2

Encrypted files

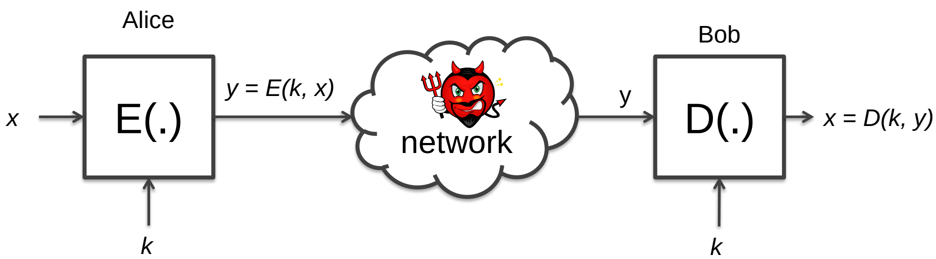


- Analogous to secure communication
- *Alice-now* sends an encrypted message to *later*

March 22 FoC - Symmetric Encryption 3

3

The model



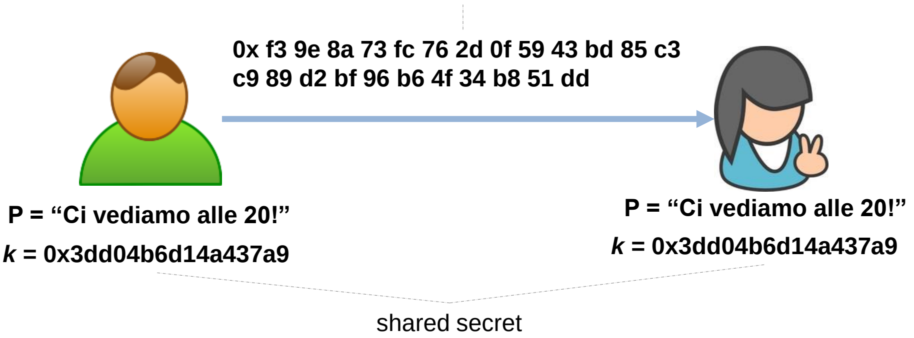
- *E*, *D*: cipher *k*: shared secret key (128 bits)
- *x*, *y*: plaintext, ciphertext

- Encryption algorithm is publicly known
  - Never use proprietary algorithm

March 22 FoC - Symmetric Encryption 4

4

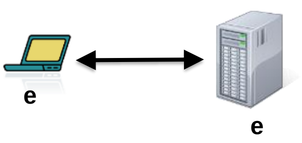
Example: DES (CBC)



March 22 FoC - Symmetric Encryption 5

5

Example: SSL



- **Handshake protocol**
  - establish a **shared secret key** by means of public key cryptography
    - 2nd part of the course
- **Record protocols**
  - use **shared secret key** to transmit data to ensure confidentiality and integrity
    - 1st part of the course

March 22 FoC - Symmetric Encryption 6

6

Cipher definition

- **(DEF)** A cipher, or encryption scheme, defined over **(K, P, C)** is a triple of “efficient” algs (Gen, Enc, Dec) s.t.
  - Gen: $\mathbf{Z}^+ \rightarrow \mathbf{K}$
  - Enc: $\mathbf{P} \times \mathbf{K} \rightarrow \mathbf{C}$; Dec: $\mathbf{C} \times \mathbf{K} \rightarrow \mathbf{P}$
  - Enc may be randomized; Dec is always deterministic
  - Equivalent notations
    - Enc(k, x), $Enc_k(x)$, E(k, x), $E_k(x)$
    - The same for Dec

March 22 FoC - Symmetric Encryption 7

7

Properties of a cipher

- Correctness
  - For all p in **P** and k in **K**, D(k, E(k, p)) = p
- Security (informal)
  - A symmetric cipher is secure iff for each pair (p, c), with p $\in$ **P** and c $\in$ **C**, then
  - given the ciphertext c, it is “difficult” to determine the corresponding plaintext p without knowing the key k, and vice versa
  - given a pair of ciphertext c and plaintext p, it is “difficult” to determine the key k, unless it is used just once

March 22 FoC - Symmetric Encryption 8

8

An historical example

Mono-alphabetic substitution

Cleartext alphabet	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Key	J	U	L	I	S	C	A	E	R	T	V	W	X	Y	Z	B	D	F	G	H	K	M	N	O	P	Q

P = "TWO HOUSEHOLDS, BOTH ALIKE IN DIGNITY,
IN FAIR VERONA, WHERE WE LAY OUR SCENE"

("Romeo and Juliet", Shakespeare)

P' = "TWOHO USEHO LDSBO THALI KEIND IGNIT
YINFA IRVER ONAWH EREWE LAYOU RSCEN E"

C = "HNZEZ KGSEZ WIGUZ HEJWR VSRYI RAYRH
PRYCJ RFMSF ZYJNE SFSNS WJPZK FGLSY S"

First Attack

- Brute force attack (exhaustive key search)
  - Oscar has ciphertext (y) and some plaintext (x)
  - Oscar tries all possible keys
    - **for each** k in K
      if (y == E(k, x)) **return** k
- The attack is *always possible*
- The attack may be more complicated because of *false positives* (later)

An historical example

- Mono-alphabetic substitution
  - The key is a permutation of the alphabet
  - Encryption algorithm
    - Every cleartext character having position *p* in the alphabet is substituted by the character having the same position *p* in the key
  - Decryption algorithm
    - Every ciphertext character having position *p* in the key is substituted by the character having the same position *p* in the cleartext
- Number of keys $\approx 26! \approx 4 \times 10^{26}$
  - number of seconds since the Universe birth!

11

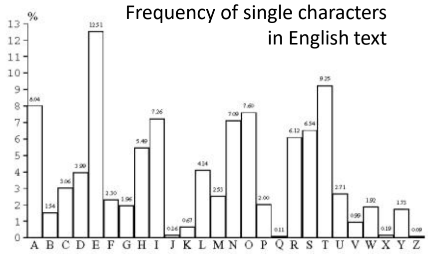
An historical example

- Brute force attack is practically infeasible given the enormous key space
- Brute force attack considers the cipher as a black box
- The monoalphabetic substitution algorithm is subject to an analytical attack which analyzes the internals of the algorithm

12

An historical example

- The monoalphabetic-substitution cipher maintains the redundancy that is present in the cleartext
- It can be “easily” crypto-analized with a ciphertext-only attack based on language statistics



Frequency of single characters in English text

An historical example

- The following properties of a language can be exploited
  - The frequency of letters
  - Generalize to pairs or triples of letters
  - Frequency of short words
    - If word separators (blanks) have been identified

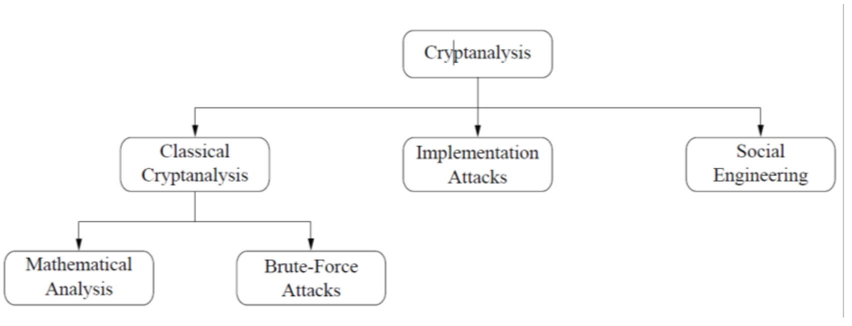
Lesson learned

- Good ciphers should hide statistical properties of the encrypted plaintext
- The cyphertext symbols should appear to be random
- A large key space alone is not sufficient for strong encryption function (necessary condition)

March 22 FoC - Symmetric Encryption 15

15

Crptanalysis



March 22 FoC - Symmetric Encryption 16

16

Attack Complexity

UNIVERSITÀ DI PISA

- Attack complexity is the dominant of:
  - Data complexity
    - Expected number of input data units required
  - Storage complexity
    - Expected number of storage units required
  - Processing complexity
    - Expected number of operations required to processing input data and/or fill storage with data

March 22 FoC - Symmetric Encryption 17

17

Types of attacks

UNIVERSITÀ DI PISA

- Attacks are classified according to what information an adversary has access to
  - ciphertext-only attack (the least strong)
  - known-plaintext attack
  - chosen-plaintext attack (the strongest)
- Fact.
  - A cipher secure against CPAs is also secure against the others
- Best practice.
  - It is customary to use ciphers resistant to a CPA even when mounting that attack is not practically feasible

March 22 FoC - Symmetric Encryption 18

18

Kerchoff's principle (19th century)

UNIVERSITÀ DI PISA

- Kerchoff's maxim
  - A cryptosystem should be secure even if everything about the system, except the key, is public knowledge
- Shannon's maxim
  - The enemy knows the system
- Pros
  - Maintaining security is easier
    - Keys are small secrets
      - Keeping small secrets, it's easier than keeping large secrets
      - Replacing small secrets, once possibly compromised, is easier than replacing large secrets

March 22 FoC - Symmetric Encryption 19

19

Security through Obscurity

UNIVERSITÀ DI PISA

- Security through Obscurity
  - Attempt to use secrecy of design or implementation to provide security
- History shows that it doesn't work
  - GSM/A1 disclosed by mistake
  - RC4 disclosed deliberately
  - Enigma disclosed by intelligence
  - ... many others…
- Defense in Depth
  - Solely relaying on StO is a poor design decision
  - StO is a valid secondary measure

March 22 FoC - Symmetric Encryption 20

20

Security through Obscurity

UNIVERSITÀ DI PISA

- "Hiding security vulnerabilities in algorithms, software, and/or hardware decreases the likelihood they will be repaired and increases the likelihood that they can and will be exploited by evil-doers. Discouraging or outlawing discussion of weaknesses and vulnerabilities is extremely dangerous and deleterious to the security of computer systems, the network, and its citizens." – S.M. Bellovin and R. Bush, *Security Through Obscurity Considered Dangerous*, Internet Engineering Task Force (IETF), February 2002.

21

Symmetric Encryption

EXERCISES

22

Shift Cipher (Caesar Cipher)

- Shift every plaintext letter by a fixed number of positions (the key) in the alphabet with wrap around
- Ex.
  - PT = «ATTACK»
  - K = 17
  - CT = “RKKRTB”

Shift Cipher (Caesar Cipher)

- Letters are encoded as numbers
  - $A \rightarrow 0$, $B \rightarrow 1$, $C \rightarrow 2$, …, $Z \rightarrow 25$
- PT, CT and K are elements of the ring $\mathbb{Z}_{26}$
  - Encryption: $y = x + k \bmod 26$
  - Decryption: $x = y - k \bmod 26$
  - EX.
    - PT (x) = «ATTACK» => 0 19 19 0 2 10
    - K = 17
    - CT (y) = 17 10 10 17 19 1 => “RKKRTB”

Shift Cipher (Caesar Cipher)

- Possible attacks
  - Brute force attack
    - Small key space: 26 possible keys
  - Anlytical attack
    - Letter frequency analysis

Affine cipher

- Definition
  - Let a, b, x, y $\in \mathbb{Z}_{26}$
  - Encryption: $y = a \cdot x + b \bmod 26$
  - Decryption: $x = a^{-1} (y - b) \bmod 26$
  - With k = (a, b) and gcd(a, 26) = 1
- Example
  - Plaintext: «ATTACK» => 0, 19, 19, 0, 2, 10
  - k = (9, 13)
  - Ciphertext: 13, 2, 2, 13, 5, 25 => «NCCNFZ»

Affine cipher

- Attacks
  - Brute force attack
    - Key space = (#values for a) × (#values for b) = 12 × 26 = 312
  - Analytical attack
    - Letter frequency analysis

27

Reader

- Understanding Cryptography, Section 1.4 “Modular Arithmetic and More Historical Ciphers”

28