Cryptography

2 homeworks: mid-november, end of the course, stuctured as the final exam.
exam 3 excercises, 2hs.
homework takes a week to complete
If it goes bad, it doesn't matter
If it goes good, 70% exam, 30% hw.
Writtn exam only exercices with open book and no theory. Oral exam no mandatory.

Katz-Lindell is a good book! Bravo me!

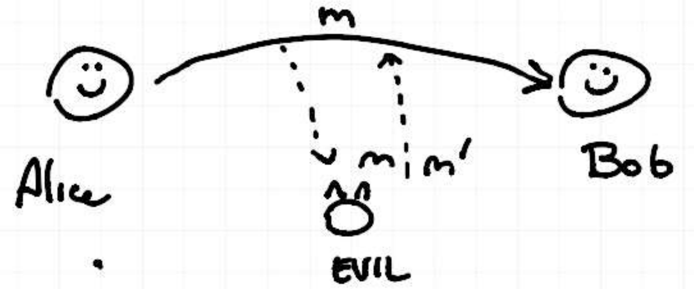
What is cryptography?

It existed in roman times and was used in the military, to carry secet communications.
Secret communications is the main reason we still use cryptography.
In the past, it was considered more as an art to hide messages in a communication and try not to get your code discovered.

Nowadays, since the '80s, cryptography became more a field in mathemathics than an art.
Secure communications are made through

provable security.

What is the problem we want to solve?
Alice and Bob want to communicate through a digital communication medium. Alice wants to send Bob a message (m) but an eavesdropper con intercept and read the message.



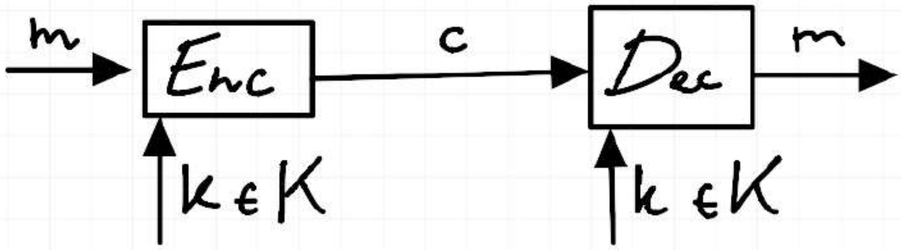
$m' \neq m$

The first goal of a secure communication is CONFIDENTIALITY, in which the eavesdropper can't listen or modify to it.
The second goal is MESSAGE INTEGRITY, so that Bob is 100% the message he receives is from Alice.

There are two kinds of solutions to the problems: SYMMETRIC CRYPTOGRAPHY is the one we will discuss in the first half of the course (ASYMMETRIC in the second)

In symmetric encryption there are two algorytms: An ENCRYPTION algorythm and a DECRYPTION one.

A message $m \in \mathcal{M}$ goes into Enc which outputs a cypertext $c \in \mathcal{C}$. c then goes into Dec and m is recovered.



The secrecy of a system does not rely on the secrecy of the algorythm, that is now public, but in the sole secrecy of the encryption key $k \in K$.

Both ends of a communication know the key (shared secret). If the key gets discovered by an eavesdropper I can just replace it without changing the algorythm.

Let's assume for now that the two parties can exchange the key in a secure way.

How can I state that the Enc algorythm is secure? Through rigourous mathematical proof!

Shannon came up with a theory of secrecy systems. The first definition is the foundation of these systems. The theory of PERFECT SECRECY

In a primitive of Enc, Dec algorythm

$$\Pi = (Enc, Dec)$$

- We want CORRECTNESS

Π is correct if

$$\forall m \in \mathcal{M}, \forall k \in \mathcal{K} : \text{Dec}(k, \overbrace{\text{Enc}(k,m)}^{c}) = m$$

- and PERFECT SECRECY

Let M be a distribution over $\mathcal{M}$, and
K be the uniform distribution over $\mathcal{K}$

all keys have the same probability

Then Π is perfectly secret if

$$\forall M, \forall m \in \mathcal{M}, \forall c \in \mathcal{C}$$

the probability of m over the probability of c

$$\Pr[M=m] = \Pr[M=m \mid C=c]$$

when $C = \text{Enc}(K,M)$ is the distribution of all possible cypertexts

This definition means that whatever key i choose, if the Π is perfectly secret, I have no information about the message from the cyphertext. If Π is not perfectly secret, I can obtain some information such as information distribution of m in c. Unfortunately, perfectly secret algorythms are not practical.

Theorem: The following are equivalent:

(i) PERFECT SECRECY

(ii) $I(M;C)=0$ (M and C are independent random variables)

(iii) $\forall m, m' \in \mathcal{M}, \forall c \in \mathcal{C}$:

$$\Pr[\mathrm{Enc}(k,m)=c] = \Pr[\mathrm{Enc}(k,m')=c]$$

(from the point of view of the attacker, c could equally likely encrypt either m or m', k is unknown to the attacker)

Proof.

We prove (i) ⇒ (ii) ⇒ (iii) ⇒ (i)

(i) ⇒ (ii)

$$\Pr[M=m] = \Pr[M=m \mid C=c] \quad \text{(by (i))}$$

$$= \frac{\Pr[M=m \wedge C=c]}{\Pr[C=c]} \quad \text{(by Beyes)}$$

$$\Rightarrow \Pr[M=m \wedge C=c] = \Pr[M=m] \cdot \Pr[C=c]$$

so (i) ⇒ (ii)

(ii) ⇒ (iii)

Fix any M, any $m \in \mathcal{M}$, $c \in \mathcal{C}$

$$\Pr[\mathrm{Enc}(k,m)=c] = \Pr[\underbrace{\mathrm{Enc}(k,M)}_{C}=c \mid M=m]$$

$$\Big\downarrow \quad = \quad \Big\uparrow \qquad = \Pr[C=c \mid M=m]$$

$$= \Pr[C=c] \quad \text{(by(ii))}$$

$$\Rightarrow \quad \Pr[\mathrm{Enc}(k,m')=c] = \Pr[C=c]$$

(iii) ⇒ (i)

Take any c from C

$$\Pr[C=c] = \sum_{m'} \Pr[C=c \wedge M=m']$$

$$= \sum_{m'} \Pr[C=c \mid M=m'] \cdot \Pr[M=m']$$

$$= \sum_{m'} \Pr[\mathrm{Enc}(k,M)=c \mid M=m'] \cdot \Pr[M=m']$$

$$= \sum_{m'} \Pr[\mathrm{Enc}(k,m')=c] \cdot \Pr[M=m']$$

$$= \sum_{m'} \Pr[\mathrm{Enc}\overset{\text{by (iii)}}{(k,m)}=c] \cdot \Pr[M=m']$$

$$= \Pr[\mathrm{Enc}(k,m=c)] \cdot \underbrace{\sum_{m'} \Pr[M=m']}_{=1}$$

$$= \Pr[\mathrm{Enc}(k,m=c) \mid M=m]$$

$$= \Pr[C=c \mid M=m]$$

$$\Rightarrow \Pr[C=c] = \Pr[C=c \mid M=m]$$

$$\Pr[M=m \mid C=c] \cdot \Pr[C=c] = \Pr[M=m \wedge C=c]$$

$$= \Pr[C=c \mid M=m] \cdot \Pr[M=m]$$

$$\Rightarrow \Pr[M=m] = \frac{\Pr[M=m \mid C=c] \cdot \cancel{\Pr[C=c]} \; \text{by } i}{}$$

~~$\Pr[C=c \mid M=m]$~~ ✓

One-Time Pad

It is a perfectly secret scheme, yet impractical.

$\Pi = (Enc, Dec) : \mathcal{K}, \mathcal{C}, \mathcal{M} = \{0,1\}^n$

XOR

$$Enc = k \oplus m$$

$$Dec = k \oplus c$$

<u>CORRECT</u> : $k \oplus (k \oplus m) = m$

Thm: OTP has perfect secrecy

Proof: we use def (iii). For all $m \in \mathcal{M}$, $c \in \mathcal{C}$

$$\Pr[Enc(k,m)=c] = \Pr[K \oplus m = c]$$

this is constant ⟶ $= \Pr[K = m \oplus c]$

$$= 2^{-n}$$

$$= \Pr[Enc(k,m')=c]$$

This proves perfect seccecy!

But what are the drawbacks?

1) $|K| = |m|$

The key is as long as the message we want to send!

2) Only one key per cyphertext

$$\left.\begin{aligned} c &= k \oplus m \\ c' &= k \oplus m' \end{aligned}\right\} \Rightarrow c + c' = m + m'$$

If I ever know m, I can easily decipher m' and all possible messages encrypted with

These drawbacks are true for all perfectly secure encryption schemes.
To be doable, we weaken the security and construct an encryption scheme that has

$|k| < |m|$

and that can use the same key for multiple messages.

Th: For any PERF. SEC. SKE,

$$|\mathcal{K}| \geq |\mathcal{M}|$$

Proof: Take M the UNIFORM DISTRIBUTION over $\mathcal{M}$

Take any $c \in \mathcal{C}$ such that $\Pr[C=c] > 0$

Consider $\mathcal{M}' = \{ Dec(k, c) : k \in \mathcal{K} \}$

Assume that $|\mathcal{K}| < |\mathcal{M}|$ (by contraddiction)

$\Rightarrow |\mathcal{M}'| \leq |\mathcal{K}| < |\mathcal{M}|$

Fix $m \in \mathcal{M} \setminus \mathcal{M}'$ (un messaggio che $\in \mathcal{M}$ ma $\notin \mathcal{M}'$)

On one hand: $\Pr[M=m] = 1/|\mathcal{M}|$

On the other hand: $\Pr[M=m \mid C=c] = \emptyset$

because $m \notin \mathcal{M}'$

$\Rightarrow$ CONTRADDICTION!

This implies that ANY perfectly secure Enc has $|\mathcal{K}| \geqslant |\mathcal{M}|$.

So our goal is to have

1) SKE with $|\mathcal{K}| << |\mathcal{M}|$

2) One Key to encrypt ALL messages