23/09/2025

INTRO TO MODERN CRYPTO

- Ceasar Cypher $(p-K) \bmod 26$ ⇝ decryption
- B4 50's ⇝ crypto was art → Secure until broken

FAM EXAMPLE: TLS (modern crypto)

└ ▷ becomes a science (not more guided by intuition and experience)

- Precise definition!
- Proofs!

TWO "FLAVOURS"

- unconditional proof (we don't care who the adversary is)
  - ▷ NO CONDITIONS/ASSUMPTIONS
  - POSSIBLE BUT INEFFICIENT ⇝ practical deployment (expensive but used for important stuff)
- conditional proof
  - ▷ WE'LL MAKE ASSUMPTIONS (Es. $P \neq NP$)

Problems that seem to be hard for efficient computation

EX: FACTORING

$n = p \cdot q$ $\quad p, q$ = primes $\quad |p| \approx |q| \approx \lambda$ bits, λ sec param.

} studied for centuries, we still fail today

- ASSUMPTION: hard to compute p, q given n

RECIPE FOR PROVABLE SECURITY. Prove this:

THM Cryptosystem X is secure if factoring is hard

Assume X not secure: ∃ efficient machine A breaking X. Then ∃ machine B solving factoring

A ⇄ B ⟵ n ⟵ p, q $\quad n = p,q$

} if it exist a machine that solve factoring. LESSSSSSSSSGO

SECURE COMMUNICATION • CONFIDENTIAL COMMUNICATION •

Alice $\xrightarrow{m \in M}$ Bob]—▷ channal to send messages ①

└ ▷ m

Eve (spiona)

• MESSAGE INTEGRITY •

Alice $\xrightarrow{m}$ Eve $\xrightarrow{m' \neq m}$ Bob ②

(stronza che cambia mess)

We have to make assumptions that Alice & Bob know smthng Alice don't know

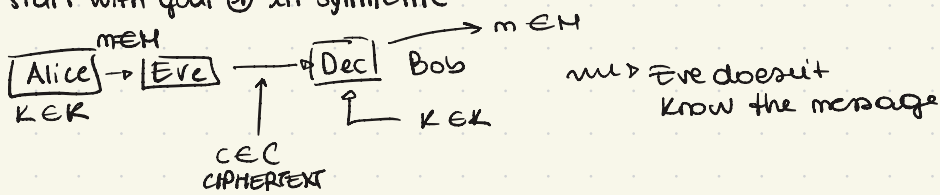
↓ → super fast

- SYMMETRIC CRYPTO: A & B share a key $K \in \mathcal{K}$; the key is random and unknown to Eve
- ASYMMETRIC CRYPTO: A e B don't share a key, but they have each their own key pair (PK, SK) where PK is PUBLIC and SK is PRIVATE

↳ Bob has to make sure the public key is Alice's & not Eve's

UNCONDITIONAL SECURITY

We start with goal ① in Symmetric



→ Eve doesn't know the message

Symmetric encryption $SKE = \Pi = (Enc, Dec)$

- $Enc : M \times K \to C$
- $Dec : C \times K \to M$
- K is uniform over $\mathcal{K}$

CORRECTNESS: $\forall K \in \mathcal{K}, \forall m \in M$

$Dec(K, Enc(K, m)) = m$

you cannot make sure the algorithm

→ instead of secretely sharing a key, A & B share an encryption method

→ KERCHOFF → Algorithms should not be secret, but publicly

Shannon (1900): def. PERFECT SECRECY

now he ben capito

DEF.:

[Enc(K,m) = m → very hard to compute the key]

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

(then observe that $C = Enc(K, M)$ as a distribution over C (cipher)

[Distrs. of message → very hard to model (Es. prob. that A sends a message at 8:00 am)]

↳ We say $(Enc, Dec) = \Pi$ is perfectly secret if $\forall M, \forall m \in M$, $\forall c \in C$ ← priory prob

$Pr[M = m] = Pr[M = m \mid C = c]$ ← posterior prob. way around to find out

← Smthing very complicated (doesn't actually tell me nothing)

Intuition: ciphertext c reveals nothing on plaintext m, beside what you know already

The prev. def. is unconditional.

Shannon → ① The def. is achievable
② It comes with inherent limitations in practice

LEMMA: The following are equivalent

(i) PERFECT SECRECY

(ii) $\mathcal{M}$ and $\mathcal{C}$ are independent) = for every pair of messages

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

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

↳ k ← uniform over $\mathcal{K}$

Let's take it as granted! (Prove it later)

How to get perfect secrecy:

The one-time PASS: $\mathcal{K}=\mathcal{M}=\mathcal{C}=\{0,1\}^n$

$Enc(k,m) = k \oplus m$

$Dec(k,m)$ $c \oplus k = (m \oplus k) \oplus k = m$

$k=0,1,1$
$n=101$ $\oplus = 1,1,0$

THM: OTP is perfectly secret

Proof. We use def 3^{iii} in lemma.

For any $m, m' \in \mathcal{M}$ and $c \in \mathcal{C}$

$P[Enc(k,m)=c]$ ← Prob. that m encrypted is = c

$= P[k \oplus m = c]$

$= P[k = m \oplus c] = 2^{-n}$ ← key lenght 2 (?)

For the same argument

$Pr[Enc(k,m')=c] = 2^{-n}$

Limitations:

- Key as long as message
- Key can only be used once (OTP)

In fact assume we encrypt m_1, m_2 with k.

$c_1 = k \oplus m_1 \; ; \; c_2 = k \oplus m_2$

$c_1 \oplus c_2 = m \oplus \oplus m_2$

If I know single pair (m_1, c_1) can compute m_2
I CAN DECRYPT ANYTHING!!!! **OTP**

THM (Shannon) Let Π be any perfectly secret SKE, then

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

Proof: Take M to be uniform over $\mathcal{M}$. Take also any ciphertext c s.t (such that)

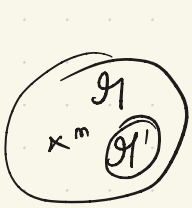
$\Pr[C=c, \mathcal{J}>0]$
↑ $Enc(k,M)$

Consider $\mathcal{M}'$ (set of all possible encryptions of c w.r.t) $\mathcal{M}' = \{Dec(k,c) : k \in K\}$
↑ cardinality

Assume $|K| < |\mathcal{M}|$ by contradiction

Then: $|m'| \leq |K| < |\mathcal{M}|$
↑ worst case: every guy has a key

$\triangleright |m'| < |\mathcal{M}|$ ← there is someone in $\mathcal{M}$ and not m'



$\Rightarrow \exists m \in \mathcal{M} \setminus \mathcal{M}'$

Now:
$\Pr[\mathcal{M} = m'] = 1/|\mathcal{M}|$

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