Goal: cryptography
- crypt. primitives → Foundations of Theoretical Crypto (P. Hubáček)
- protocols
- implementation

Why? ① understand existing protocols
② design of protocols

Exam: ① theory
② protocol to break

Symmetric Encryption

Who are A + B?

Mallory
man in the middle
active attacker

plaintext: Alice → E → ciphertext → D → Bob (plaintext)

encryption: K → E; K → D

↳ Eve, passive attacker

Formally: $E: \{0,1\}^n \times \{0,1\}^k \to \{0,1\}^n$

(plaintext, key, ciphertext)

$E(X,K) = Y \qquad E_K(X) = Y$

$D: \{0,1\}^n \times \{0,1\}^k \to \{0,1\}^n$

$D(Y,K) = X$

$\forall K\ \forall X \quad D(E(X,K),K) = X$

for fixed K: $\mathcal{U} \xrightarrow{E_K} \mathcal{U}$

E_K as a permutation on $\{0,1\}^n$
"random"

Kerckhoffs Principle: Secret should be the key, not the algorithm.

Reasons: ① good ciphers are hard to find
② public standards are well studied
③ keys are easier to change if compromised

(Silly) Example: Ceasar's Cipher
messages: $\{0, \ldots, 25\}$ $\mathbb{Z}_{26}$
keys: $\mathbb{Z}_{26}$
$E(X,K) = X + K \qquad D(Y,K) = Y - K$

Asymmetric Cipher

$D(E(X, K_E), K_D) = X$

Alice → E → D → Bob

K_E → E; K_D → D

(K_E, K_D) ↑ key gen.

① Multi-party comm. network
n pairs of keys
- K_E's public
- K_D's private

A → B: K_E^{Bob}, K_D^{Bob}

n people

catch: key distribution

② Signature Scheme

A → Sign → signed msg → verify → plain text

K_{Sign}^A private; K_{Verify}^A public

n pair of keys
- K_E's private (signing key)
- K_D's public (verif. key)

Hash Function

fixed (e.g., 256) ~ 2^{78}

$h: \{0,1\}^* \to \{0,1\}^b$
"random"

RSA (k_1, k_2)

① impossible to invert.
given y, cannot find x: $h(x) = y$

② impossible to find collisions:
$x \neq x'$: $h(x) = h(x')$

Applications:

① signatures

A wants to sign X:
- send X in plaintext
- $E(h(X), K_{sign}) \longrightarrow D(-, K_{ver.})$

② Challenge-response authentication

A user (Password) ← challenge ← B server (Password)
data → $h(\text{challenge} \,\|\, \text{password} \,\|\, \text{data})$

SCRAM

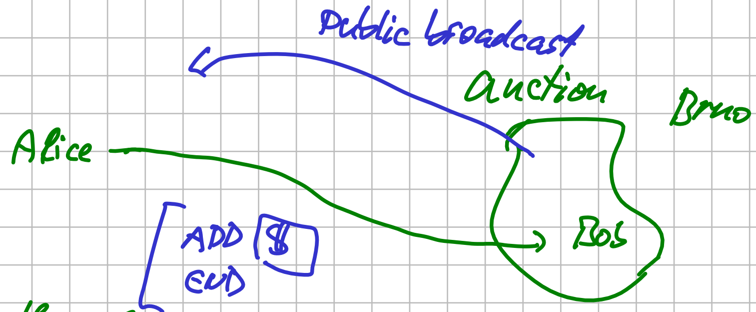
Challenge: random X nonce

Random Generator

- unpredictable
- cannot be influenced

Combine Sym. & Asym Cipher
gen. K_{SYM} random (per message) 256 bit
send: $E_{SYM}(X, K_{SYM})$, $E_{ASYM}(K_{SYM}, K_{ENC})$

1. Auction Protocol



2. Tossing a coin over the phone