Cryptography

- Symmetric-key (*)
  (Private key)
- Public-key

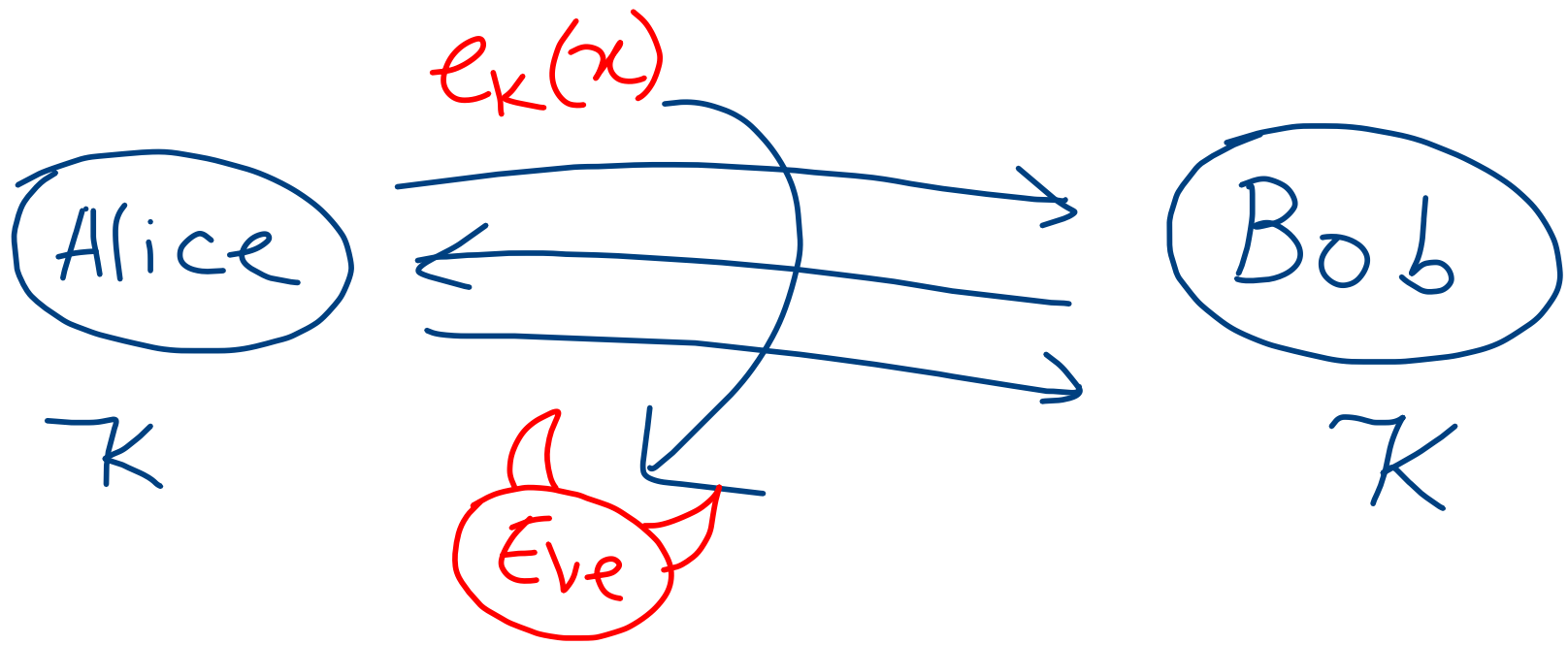
→ Krypto → hidden
Graphene → writing

Cryptology

Cryptography

Cryptanalysis

Symmetric-key Cryptography



- Both Bob, Alice share a key (K) → Secret
- Kerchoff's law: "Only key is the secret".

Classical Ciphers

Cryptosystem:

$$(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$$

- $\mathcal{P}$: set of plaintexts
- $\mathcal{C}$: Set of ciphertexts
- $\mathcal{K}$: set of keys
- $\mathcal{E}$: encryption rules
- $\mathcal{D}$: decryption rules

$\forall k \in \mathcal{K}$,

$\mathcal{E}_k : \mathcal{P} \to \mathcal{C}$

$\mathcal{D}_k : \mathcal{C} \to \mathcal{P}$

Correctness: $\mathcal{D}_k(\mathcal{E}_k(x)) = x, \ \forall x \in \mathcal{P}, \ \forall k \in \mathcal{K}$

Shift Cipher

$\mathcal{P} = \mathbb{Z}_{26}$

$\mathcal{C} = \mathbb{Z}_{26}$

$\mathcal{K} = \mathbb{Z}_{26}$

$e_k(x) = (x + k) \bmod 26$

$d_k(y) = (y - k) \bmod 26$

Alternate Representation

$\mathcal{P} = \mathbb{Z}_{26}^{\ell} = \mathcal{C}$

$\mathcal{K} = \mathbb{Z}_{26}$

$e_k(x_1 \ldots x_\ell) = (x_1 + k \bmod 26, \ldots, x_n + k \bmod 26)$

A → 0
B → 1
⋮
Z → 25

$x_1 x_2 x_3 \ldots\ldots x_n$

$e_k(x_1)\ e_k(x_2) \ldots\ldots e_k(x_n)$

Hello

↓ K=3

Khoor

Caesar Cipher

Shift Cipher with K=3

Substitution Cipher

$P = C = \mathbb{Z}_{26}$ $\quad K =$ Set of all permutations of $\{0, 1, \ldots, 25\}$

$e_k(x) = k(x)$

Mono-Alphabetic

π_8:

0	1	2	. . .	25
6	11	17		0

$e_{\pi_8}(2) = 17$

Substitution Cipher

$P = C = \mathbb{Z}_{26}$ $\quad K =$ Set of all permutations of $\{0, 1, \ldots, 25\}$

$e_k(x) = k(x)$

key-space $= 26!$

$\approx 2^{78}$

π_8:

0	1	2	. . .	25
6	11	17		0

$e_{\pi_8}(2) = 17$

Affine Cipher

$P = C = \mathbb{Z}_{26}$

$K = \mathbb{Z}_{26} \times \mathbb{Z}_{26}$

$e_{(a,b)}(x) = \{(ax+b) \bmod 26 \mid \gcd(a,26) = 1\}$

$d_{(a,b)}(y) = a^{-1}(y-b) \bmod 26$

$\#keys = 26 \times \underline{12} = 312$

$\phi(26)$

Why?

$y = (ax+b) \bmod m$

unique x iff

$\gcd(a,m) = 1$

Vigenere Cipher

$$\mathcal{P} = C = \cancel{K} = \mathbb{Z}_{26}^{m}$$

$$e_k(x) = (x + k) \bmod 26$$

$$x = x_1 x_2 \cdots x_m$$
$$\downarrow$$
$$\in P$$
$$\Downarrow$$
$$x = x_1 x_2 \cdots x_n$$
$$\downarrow$$
$$x_i \in \mathbb{Z}^m$$

Example:

$m = 3$ (KEY: ABC)

PT: CRYPTOLOGY

KEY: ABCABCABCA

CT: D R Q

Poly-Albhatic Cipher

- Hill Cipher

$P = C = \mathbb{Z}_{26}^m \quad K \to \{m \times m \text{ inv matrix}\}$

$e_K(x) = x \cdot K$

$m \times m$ - matrix

- Permutation Cipher

$P = C = \mathbb{Z}_{26}$

$K \to$ Permutations of $\{0, 1, \ldots, 25\}$

$e_K(x_1 x_2 \ldots x_m) = x_{K(1)} x_{K(2)} \ldots x_{K(m)}$

Cryptanalysis of Vigenere Ciphers

- $y = y_1\ y_2 \cdots - \ y_n$
- You have found m
- $n = r \cdot m$