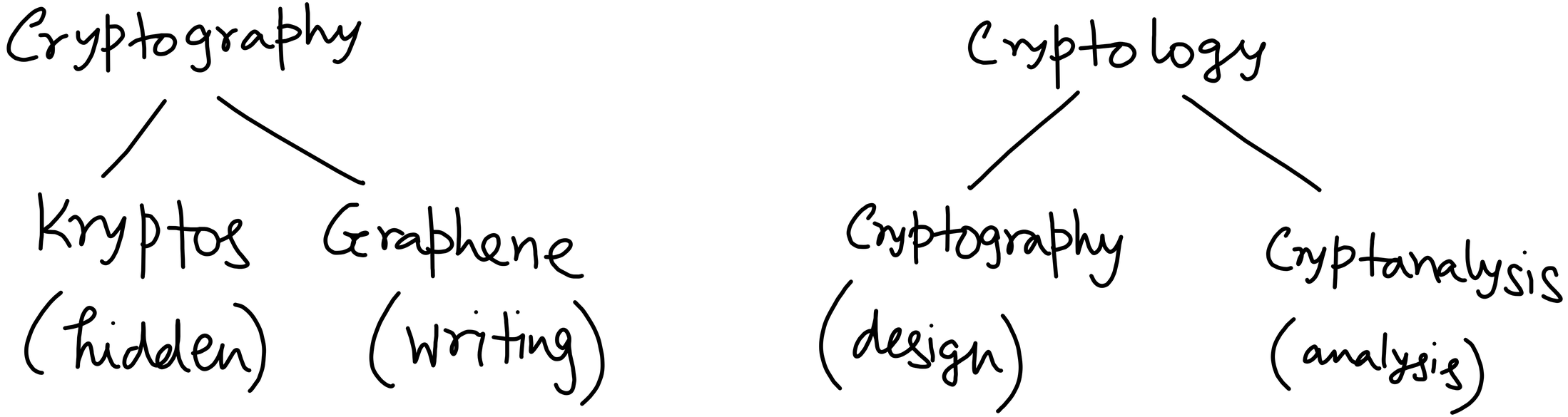
Cryptology


Cryptography
Kryptos
(hidden)
Graphene
(writing)
Cryptology
Cryptography
(design)
Cryptanalysis
(analysis)

Enigma

└ Second world war.

Kerchoff's Principle: Only key is the secret, everything else is known.

$$\mathcal{E} : \mathcal{K} \times \mathcal{P} \rightarrow \mathcal{C}$$

$$\mathcal{D} : \mathcal{K} \times \mathcal{C} \rightarrow \mathcal{P}$$

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

- $\mathcal{E}_k(\cdot)$ → Should be a permutation.

Correctness:

$\forall k \in \mathcal{K}$, $\forall m \in \mathcal{P}$ $\quad \mathcal{D}_k(\mathcal{E}_k(m)) = m$.

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

$\mathcal{P}$: Set of Plaintexts

$\mathcal{C}$: Set of Ciphertexts

$\mathcal{K}$: Set of keys

$\mathcal{E}$: Encryption func

$\mathcal{D}$: Decryption func

Shift Cipher

$m =$ hello

$k =$ 11111

$c =$ ifmmp

Shift cipher with key $k = 1$

Shift Cipher

$m =$ hello

$k =$ 11111

$c =$ ifmmp

Shift cipher with key $k = 1$

- $\mathcal{M} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_{26} = \{0, 1, \ldots, 25\}$
- $\mathcal{E}_k(m) = (m + k) \bmod 26$
- $\mathcal{D}_k(m) = (m - k) \bmod 26$

$$\mathcal{E}_k(m_1 \ldots m_n) = \mathcal{E}_k(m_1) \| \mathcal{E}_k(m_2) \| \ldots$$

Symmetric / Private Key Cryptography

- Sender & receiver has a shared secret key.

Asymmetric / Public-Key Cryptography

Sender → (SK_S, PK_S)

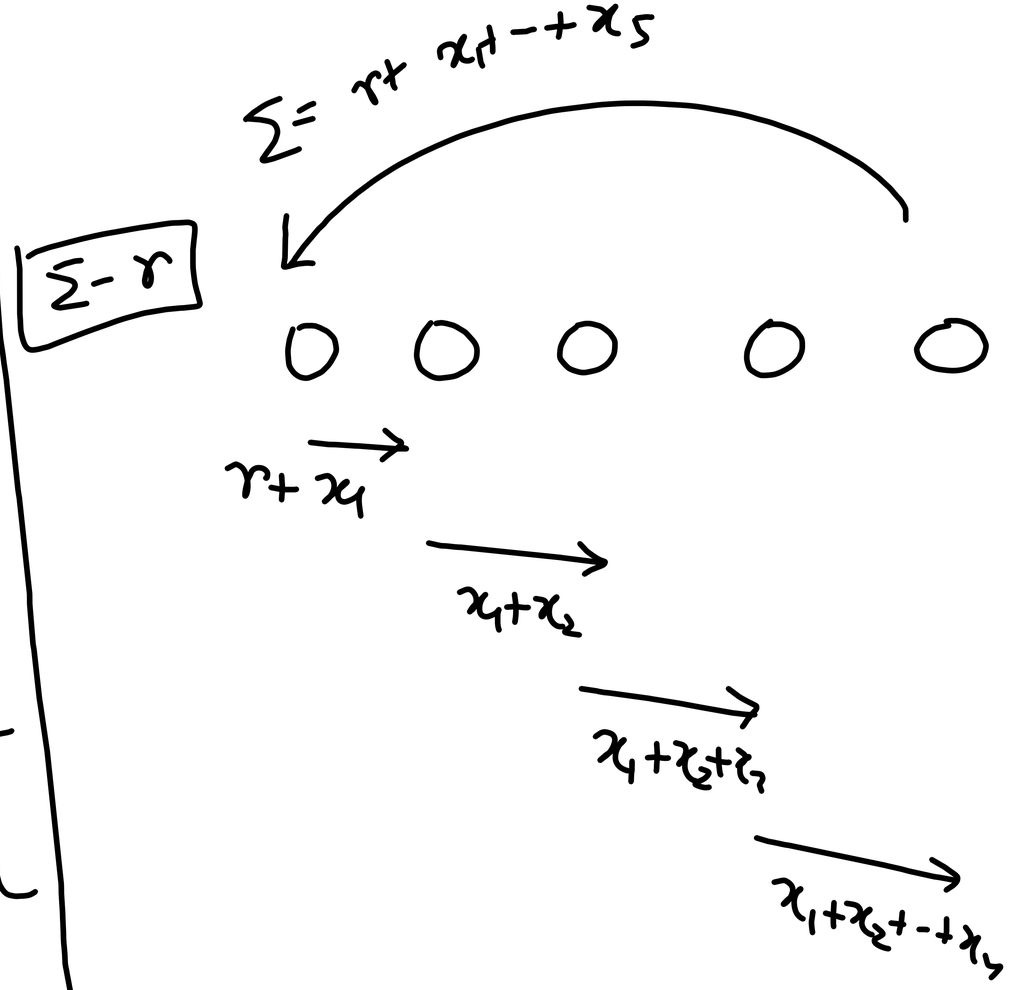
Receiver → (SK_R, PK_R)

$$C = Enc_{PK_R}(m)$$

$$m = Dec_{SK_R}(C)$$

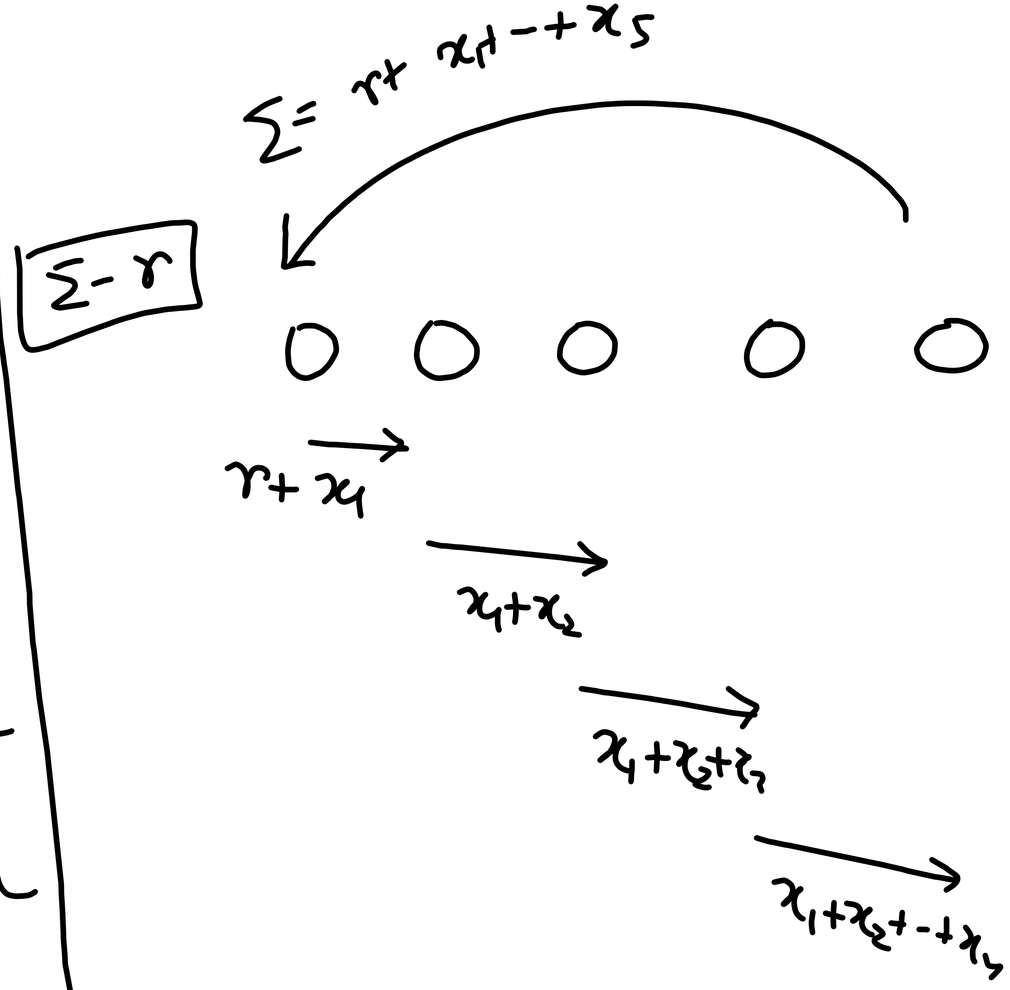
Real-Life Applications

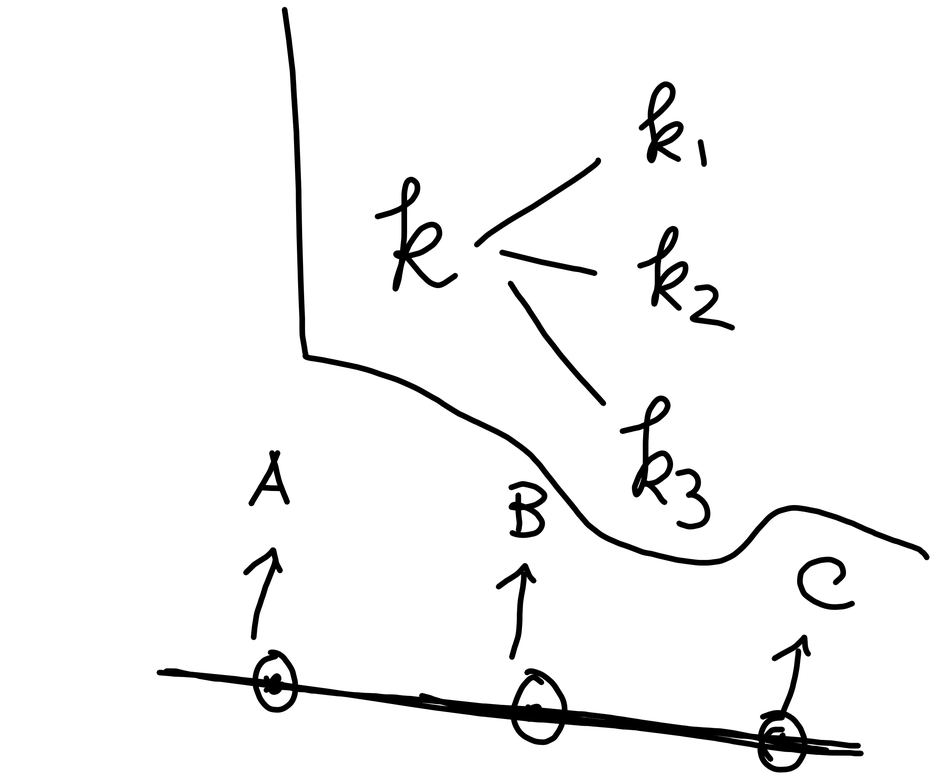
- Confidentiality / Privacy
- Integrity / Authentication
- Authenticated Encryption
- Multi-party Computation



Real-Life Applications

- Confidentiality / Privacy
- Integrity / Authentication
- Authenticated Encryption
- Multi-party Computation
- Secret sharing
- Zero Knowledge Proof





$k_1, k_2 \rightarrow k$

$k_1, k_3 \rightarrow k$

$k_2, k_3 \rightarrow k$

$y = mx + c$

Constant (key)