# Classical Ciphers

## Shift Cipher

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

$$E_k(m) = (m + k) \bmod 26.$$

$$D_k(c) = (c - k) \bmod 26.$$

# Affine Cipher

Frequency of letters

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

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

$$\mathcal{E}_{a,b}(x) = ax + b \bmod 26$$

$$\Rightarrow \mathcal{D}_{a,b}(y) = a^{-1}(y-b) \bmod 26$$

$$K = \phi(26) \times 26$$
$$= 12 \times 26$$
$$= 312$$

$y = ax + b$

$ax = y - b$

$x = a^{-1}(y-b)$

$\Rightarrow$ $\boxed{\gcd(a, 26) = 1}$

$\Downarrow$ (iff)

$a^{-1}$ unique

## Shift, Affine Cipher

↳ Key space should be large.

## Substitution

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

$\mathcal{K}$ = Any permutation of 26 no.

$\mathcal{E}_k(m) = K(m)$, where $k \in Perm(26)$

$\mathcal{D}_K(m) = K^{-1}(m)$.

Key Space → 26!

≈ $2^{88}$

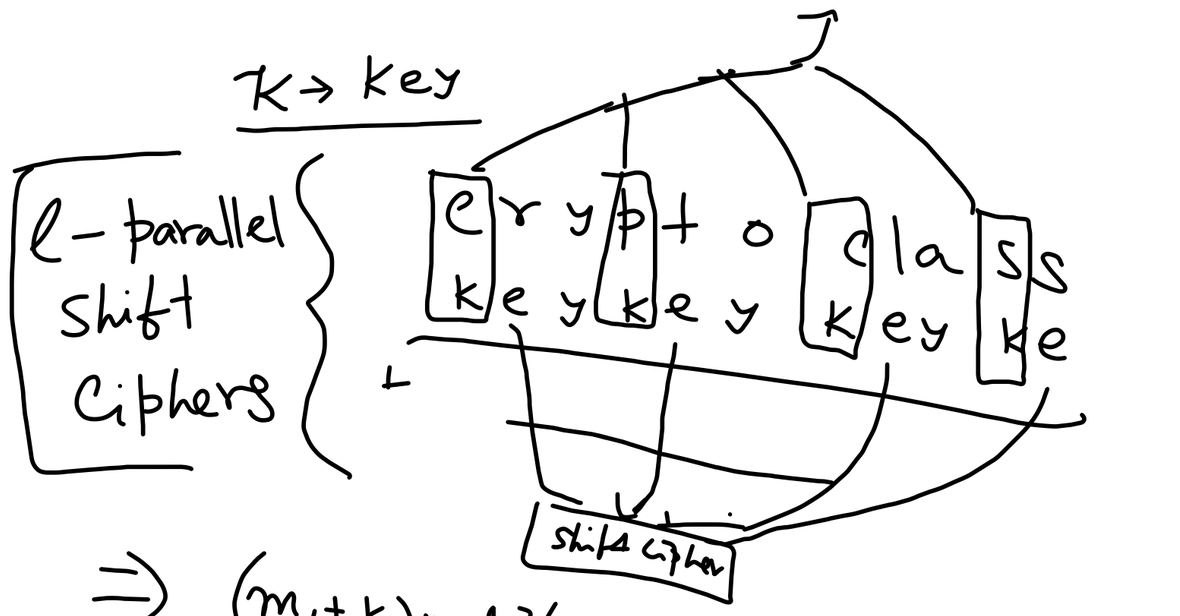
# Mono-alphabetic Cipher

↳ fixed mapping of alphabets.

# Vigenere Cipher

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

$$\mathcal{E}_k(m) = (m + k) \bmod 26 \Rightarrow (m_1 + k_1) \bmod 26, \ldots\ldots, (m_\ell + k_\ell) \bmod 26$$




(Poly-Alphabetic Cipher)

↳ multiple mapping is possible for each alphabet

Classical Ciphers $\Longrightarrow$ Modern Ciphers

1) Concrete Definition of Security

2) Underlying assumptions

3) Proofs

} Modern Cryptography

# Definition of Security

## Goal

1. Difficult to get key. (Key Recovery)
2. Plaintext Recovery
3. No meaningful information Can be obtained
4. No additional information is obtained from the ciphertext

## Attack Model / Power of Adversary

1. Ciphertext-only (CA)
2. known-Plaintext (KPA)
3. Chosen Plaintext (CPA)
4. Chosen Ciphertext (CCA)

# Assumptions

- Clearly mention your underlying assumptions.
- Try to use well studied assumptions.

# Proof

- Goal
- Power of adv
- Assumptions

} $\mathcal{E}$ is secure.

# Index of coincidence

| P/T | C/T |
|---|---|
| $p_1$ | $q_1$ |
| $p_2$ | $q_2$ |
| ⋮ | ⋮ |
| $p_{26}$ | $q_{26}$ |

$$\left\{ I_C = \sum_{i=1}^{26} p_i^2 \right.$$

$Pr[a] = p_1$

$Pr[b] = p_2$

⋮

$Pr[z] = p_z$

## Shift Cipher

⇓

$k=0 \Rightarrow (p_1q_1 + p_2q_2 + \cdots + p_{26}q_{26})$

$k=1 \Rightarrow (p_1q_2 + p_2q_3 + \cdots + p_{26}q_1) = I_C$

⋮

$k=25 \Rightarrow (p_1q_{26} + p_2q_1 + \cdots + p_{26}q_{25})$

| $p_1$ | $p_2$ | $p_3$ |
|---|---|---|
| 0.8 | 0.1 | 0.1 |

$I_C = 0.64 + 0.01 + 0.01$

$= 0.66$

$0.8 \times 0.1 + 0.1 \times 0.8 + 0.1 \times 0.1$

$= 0.08 + 0.08 \times 0.01$

$= 0.17$