

4F5: Advanced Communications and Coding

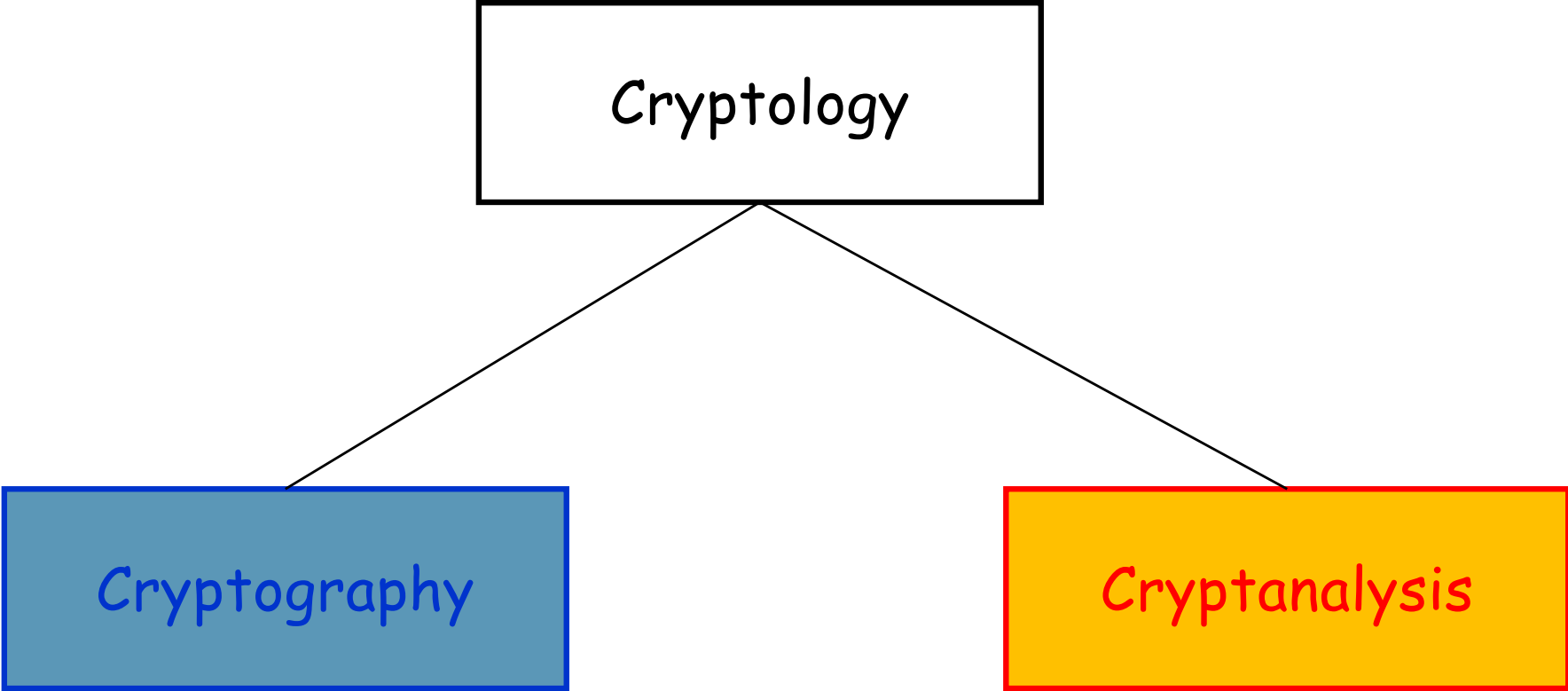
Cryptology

Jossy Sayir and Jim Massey 

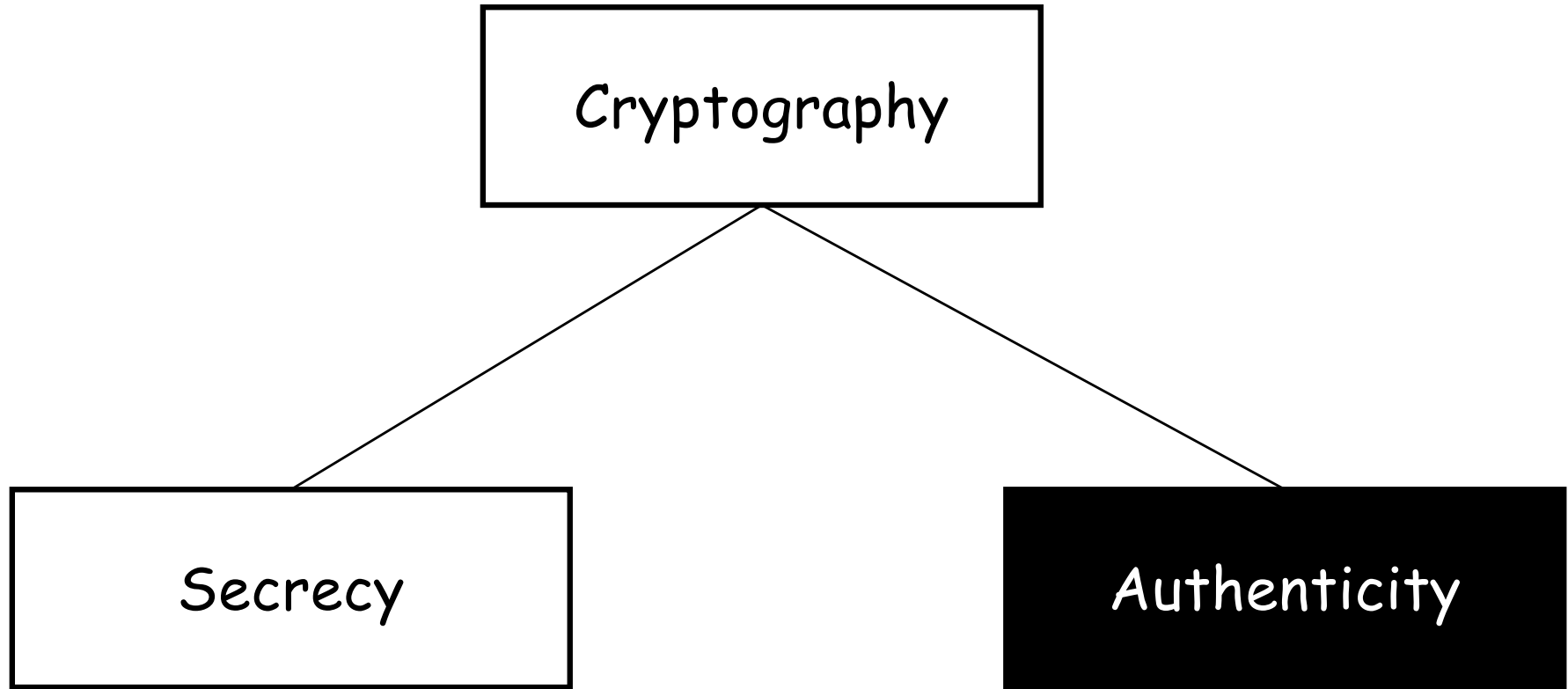
Probabilistic Systems, Information and Inference Lab
Dept. of Engineering
jossy.sayir@eng.cam.ac.uk

Lent Term 2026

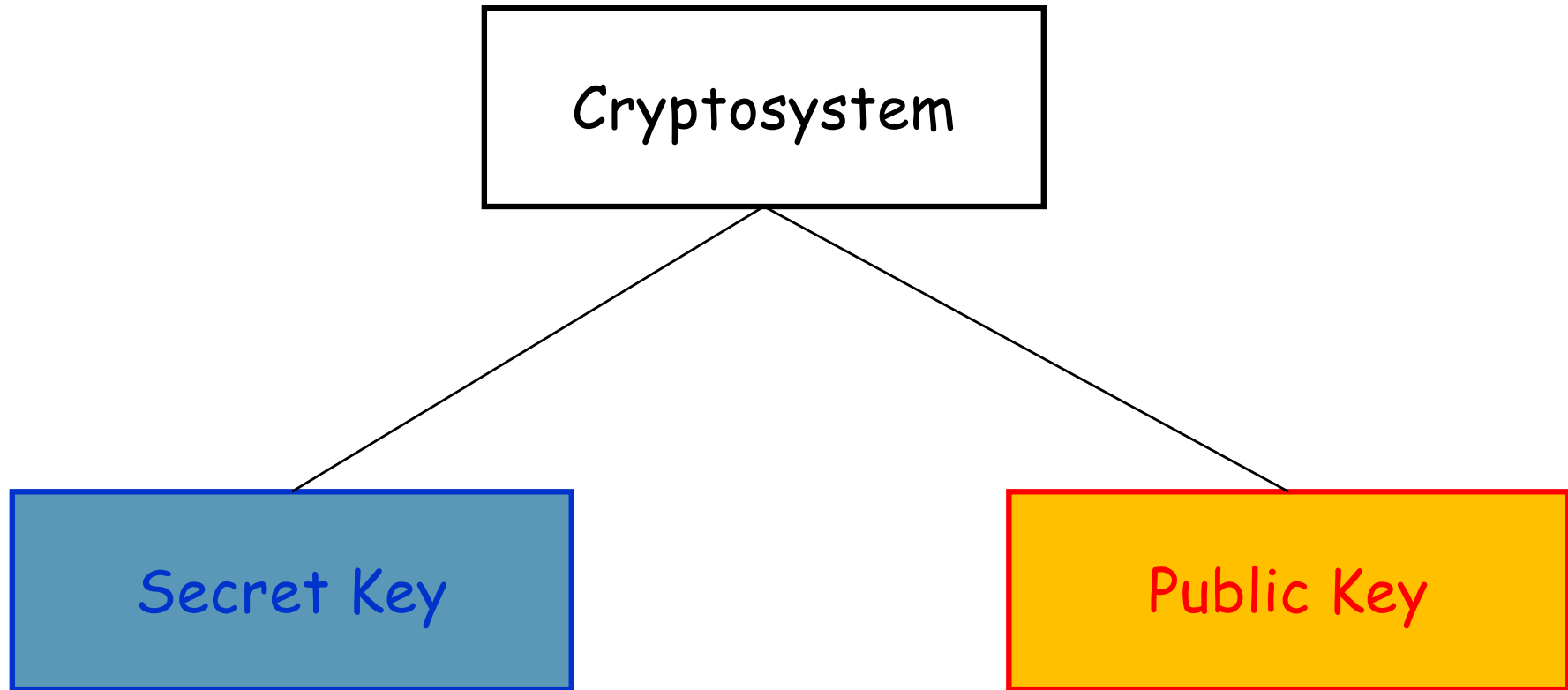
Definitions



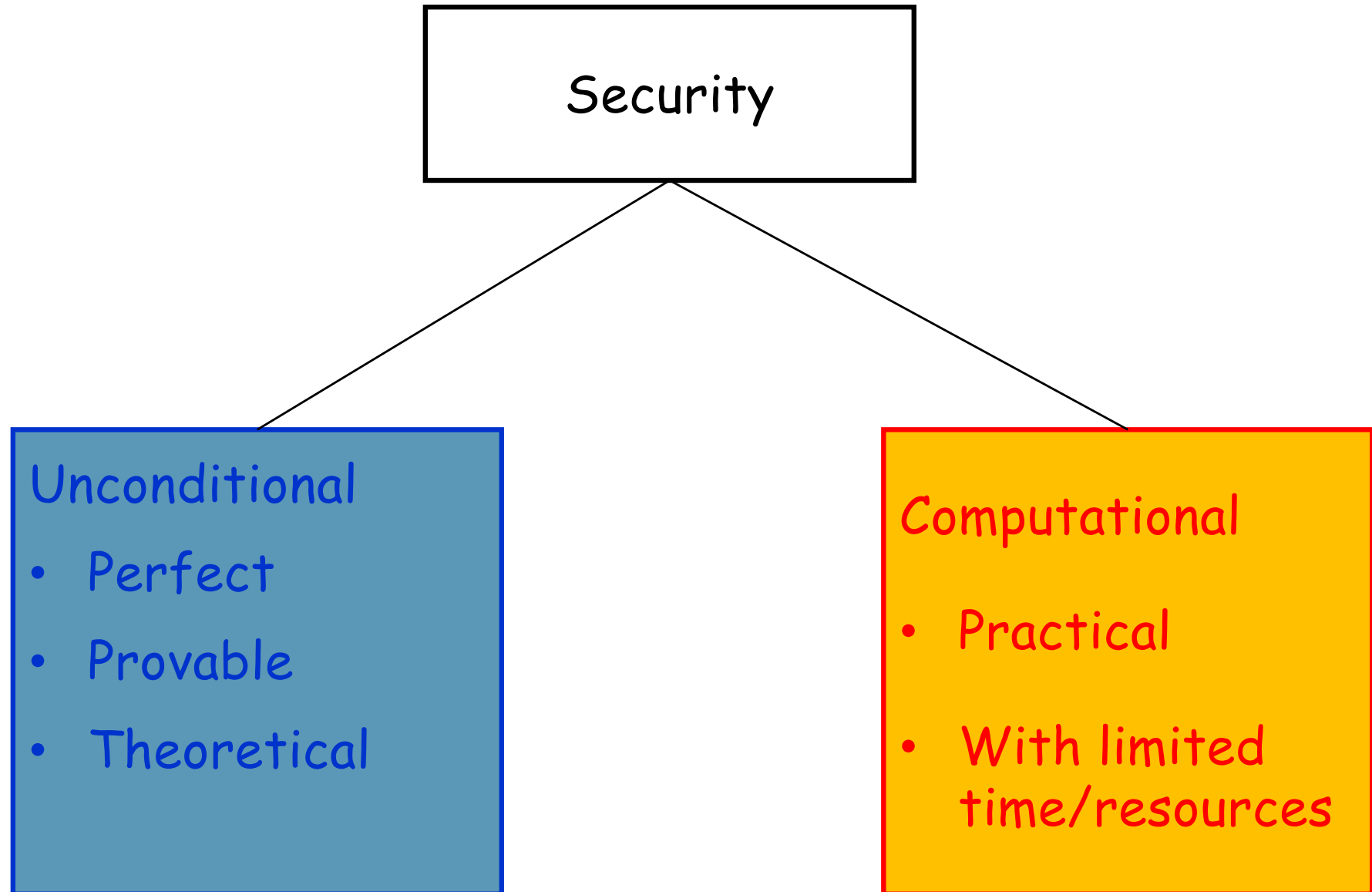
Goals of Cryptography



Cryptographic Systems



Cryptographic Security



Cryptanalytic attacks

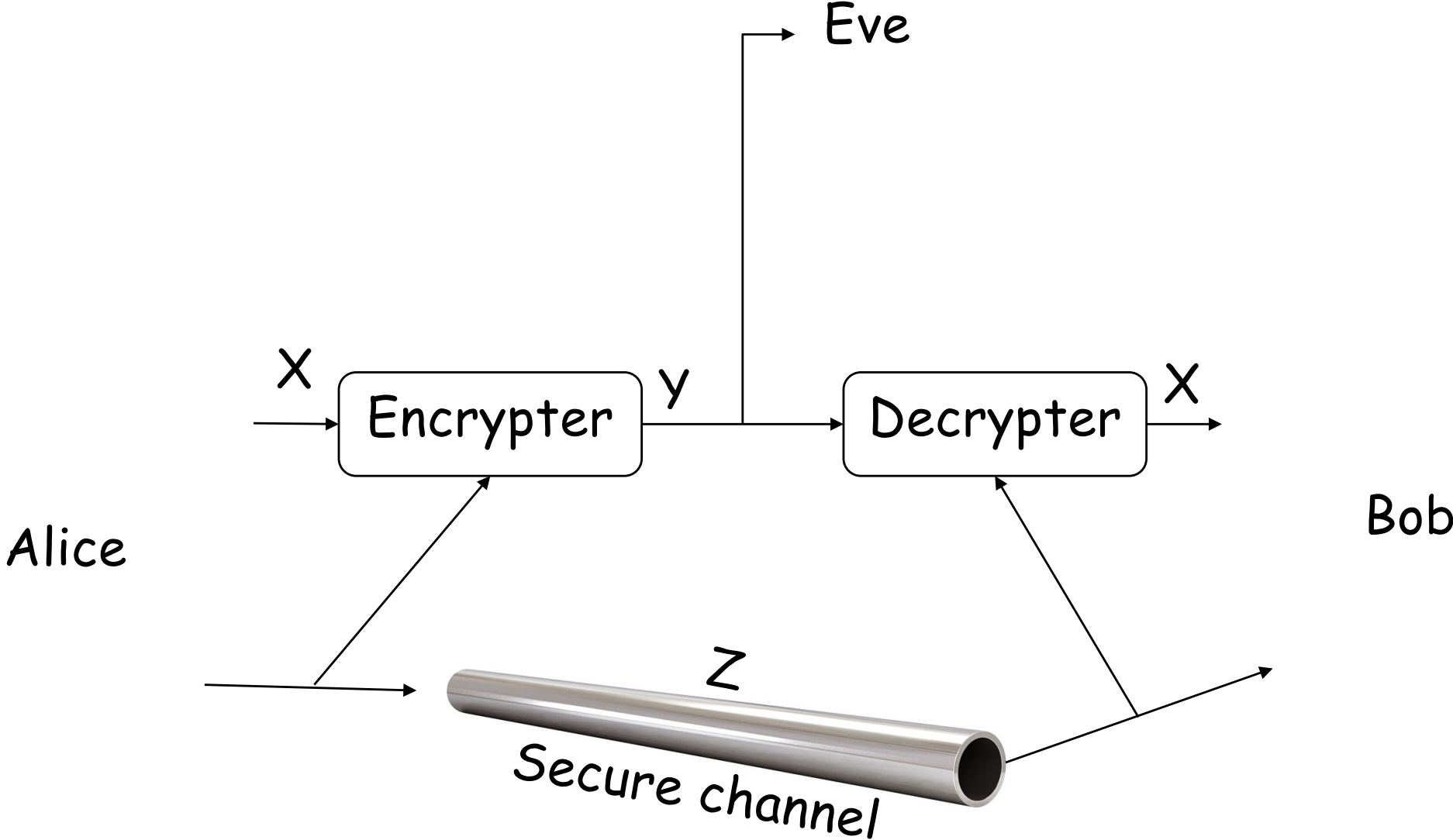
- **Ciphertext only** attack
- **Known plaintext** attack
- **Chosen plaintext** attack
- **Chosen ciphertext** attack

Kerckhoffs' principle

The cipher should be designed so as to be secure when the enemy cryptanalyst knows all details of the enciphering process and deciphering process except for the secret key.

August Kerckhoffs, 1835-1903

General Model of a Secret Key System



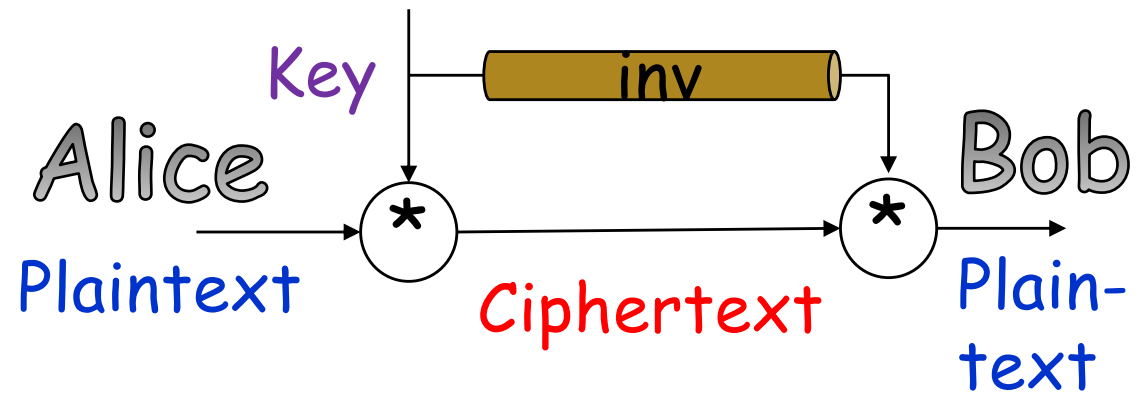
Shannon's Perfect Secrecy

- **Encryptability:** $H(Y|X,Z) = 0$
- **Decryptability:** $H(X|Y,Z) = 0$
- **"Perfect" secrecy:** $I(X;Y) = H(X) - H(X|Y) = 0$
- **Shannon's theorem:** perfect secret systems exist with $H(Z) \geq H(X)$
- You need **more bits of key** than **secret text**

Caesar's cipher

- Add k modulo 26 to each letter
- Example, $k=3$
- HELLO WORLD
↑↓ ↑↓ ↑↓ ↑↓ ↑↓ ↑↓ ↑↓ ↑↓ ↑↓
- KHOOR ZRUOG
- far from perfect...

One-time-pad (Vernam's Cipher)

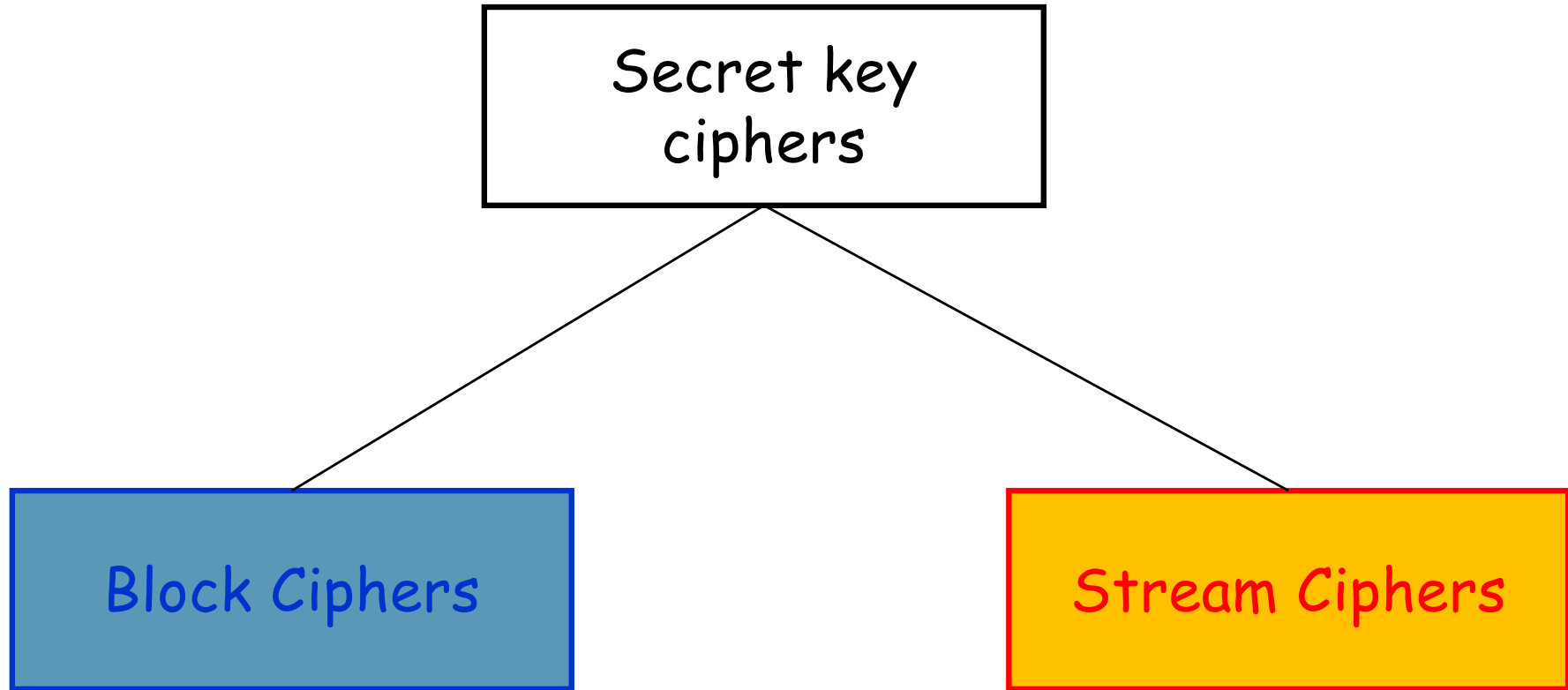


- Plaintext in a group $\langle G, * \rangle$ of order m
- Secret key is a string of uniform and independent random symbols in G of same length as plaintext
- **Ciphertext** = Plaintext * Key
(element-wise group operation)
- **Decrypted text** = Ciphertext * Key⁻¹
(element-wise group operation with inverse)

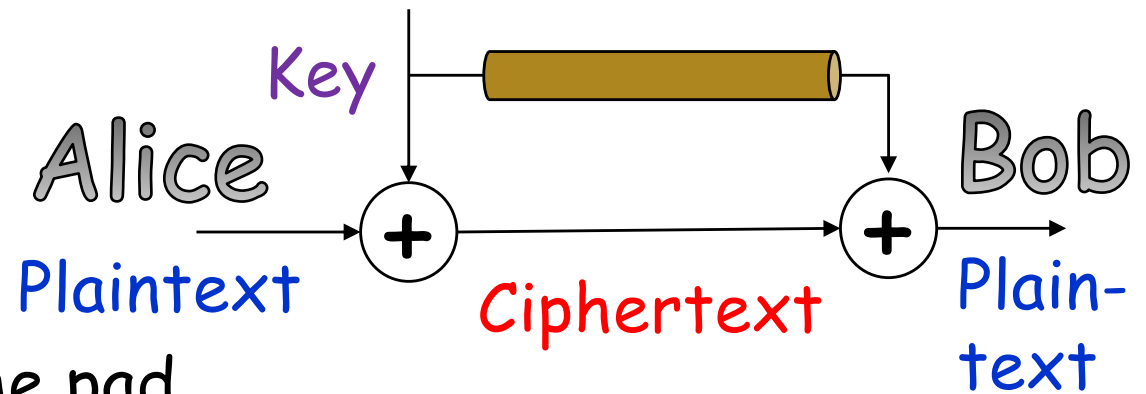
Perfect Secrecy

- Vernam's cipher / one time pad offers **perfect secrecy in Shannon's sense**.
- It is deemed "impractical" because it requires a large common key
- However, there are many applications where it is very practical. Conspiracy theories about the NSA/KGB/GCHQ or whatever the agencies are called being able to crack every cryptosystem are wrong: we have a mathematical proof in this case!

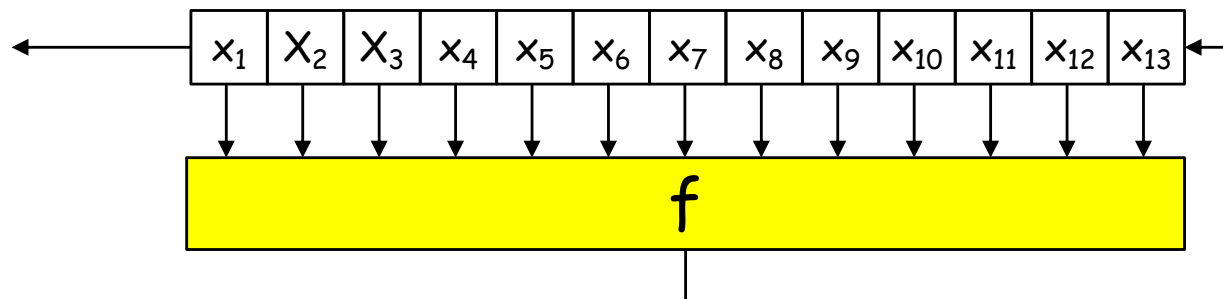
Secret Key Ciphers



Stream Ciphers



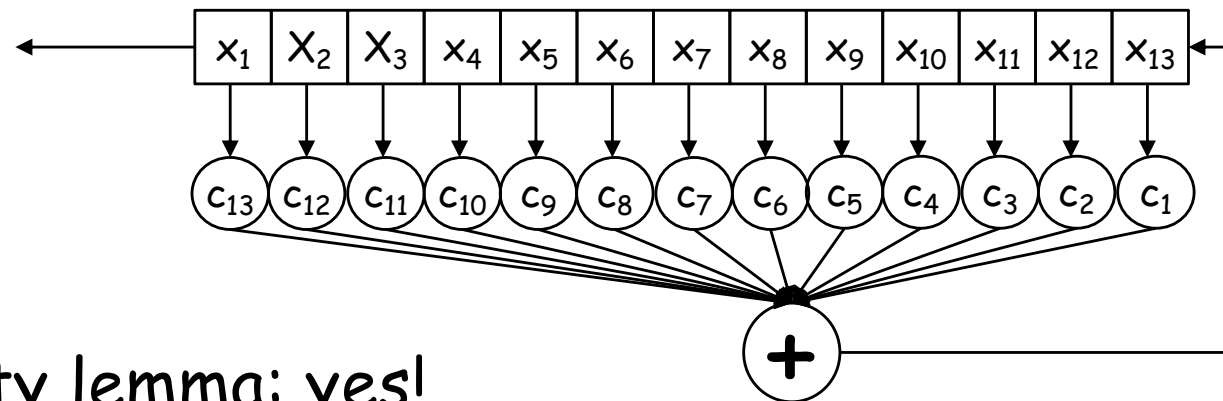
- Inspired by one-time pad
- Key is "pseudo-random", produced by a "Running Key Generator" (RKG)
- Typical RKG:



- x_n can be m -ary symbols, f is typically a non-linear function of \mathbb{Z}_m^k to \mathbb{Z}_m

Running Key Generators

- Is the sequence produced by an RKG periodic?
- Periodicity lemma: yes!
- Can the sequence be generated by a Linear Feedback Shift Register / Recurrence Relation?

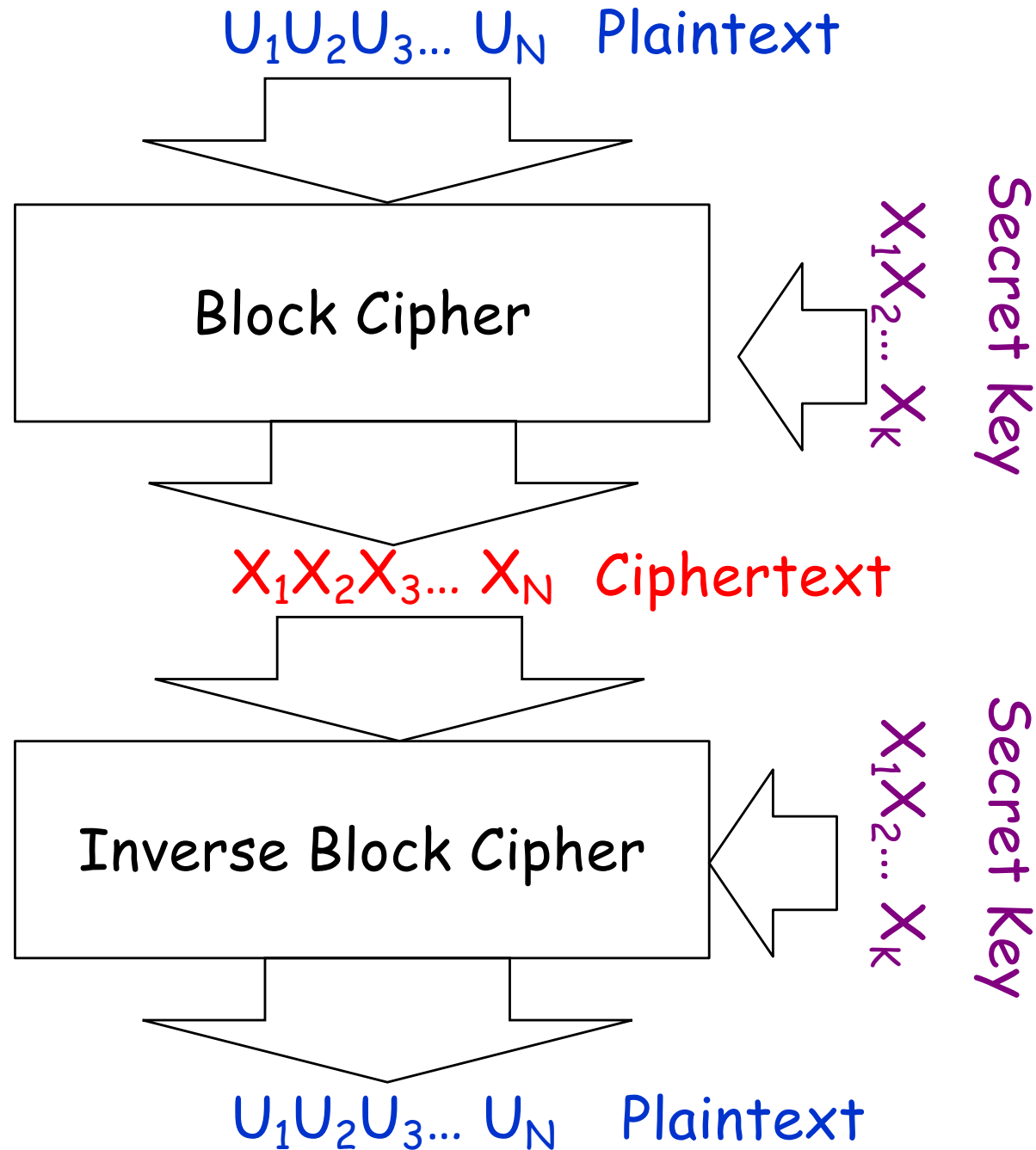


- Linearity lemma: yes!
- Every periodic sequence of period P over \mathbb{Z}_m has a finite linear complexity $\mathcal{L} < P$

Stream Cipher design

- LFSR in stream ciphers: $X(z)C(z) = P(z)$
- $C(z)$ coefficients known, $P(z)$ is the additive RKG sequence. Known plaintext attack: guess $X(z)$.
- Problem is equivalent to Reed Solomon decoding...
- LFSRs can be used in stream ciphers but usually not on their own as they are weak
- Even when using non-linear feedback registers, pick ones that have a *high linear complexity*, or they can be attacked via Berlekamp-Massey (efficient LFSR constructor developed for Reed-Solomon decoding)
- Enigma (German WWII cipher) is a stream cipher
- Stream ciphers in common use today for military and civilian applications!

Block ciphers



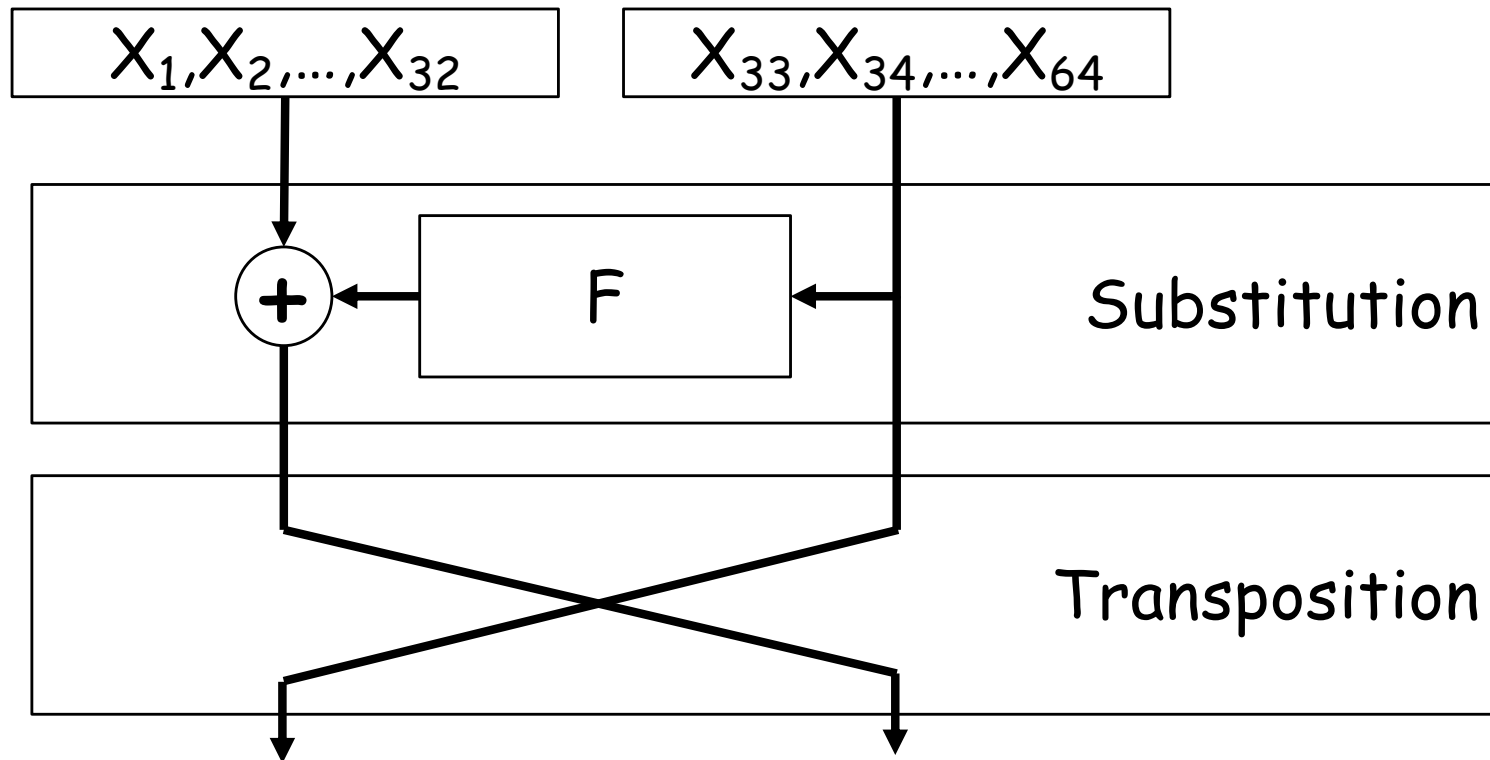
Block cipher principles (Shannon, 1949)

- **Confusion:** ciphertext statistics should not depend in an obvious manner on the plaintext statistics
- **Diffusion:** each symbols of plaintext or key influences as many symbols of ciphertext as possible

Types of block cipher components

- **Substitution** element: substitutes each symbol (where "symbol" can mean a block of digits) by another symbol in a bijective manner (i.e., permutation of the *alphabet!*)
- Maintains source statistics as long as key is not changed, but offers good **confusion** in short blocks.
- **Transposition** element: re-orders symbols in a block (i.e., permutation of the *locations!*).
- Breaks up local dependencies and hence gives good **diffusion**

Data Encryption Standard



1 of 16 rounds
F is Feistel function $F(X,K)$
Invertible structure!

History of Block Ciphers

- DES was a standard commissioned by the US National Bureau of Standards 1976 based on Lucifer, developed by Horst Feistel at IBM in the 1970s. It is no longer considered safe (56 bits of effective key, can be broken by exhaustive search!)
- IDEA developed by Lai & Massey (ETH Zurich) in 1991
- RC5 developed by Ron Rivest (MIT) in 1994
- AES standard adopted by NIST in 2001 based on Rijndael developed by Rijman & Daemen in Belgium

Public Key Cryptography

- Can two parties agree on a **secret key** in full **public view**, so that by the end of the transaction only the two parties know the key despite the fact that the public intercepted all communications between them?
- Public key cryptography: protocols to provide computational security (secrecy and authenticity) based on one-way functions and trapdoor one-way functions.