ICT Course: Introduction to Cryptography

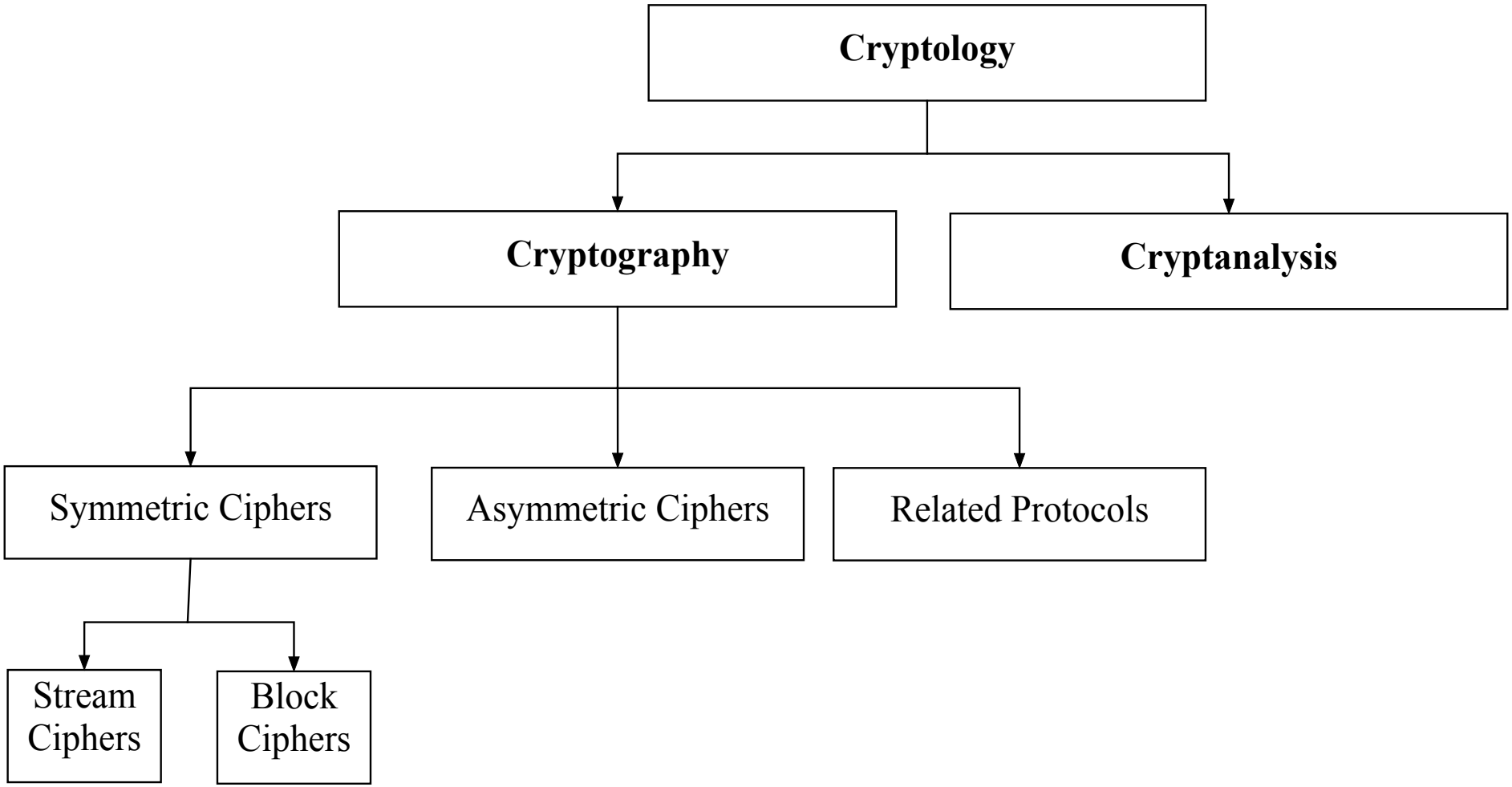
Nguyen Minh Huong

ICT Department, USTH

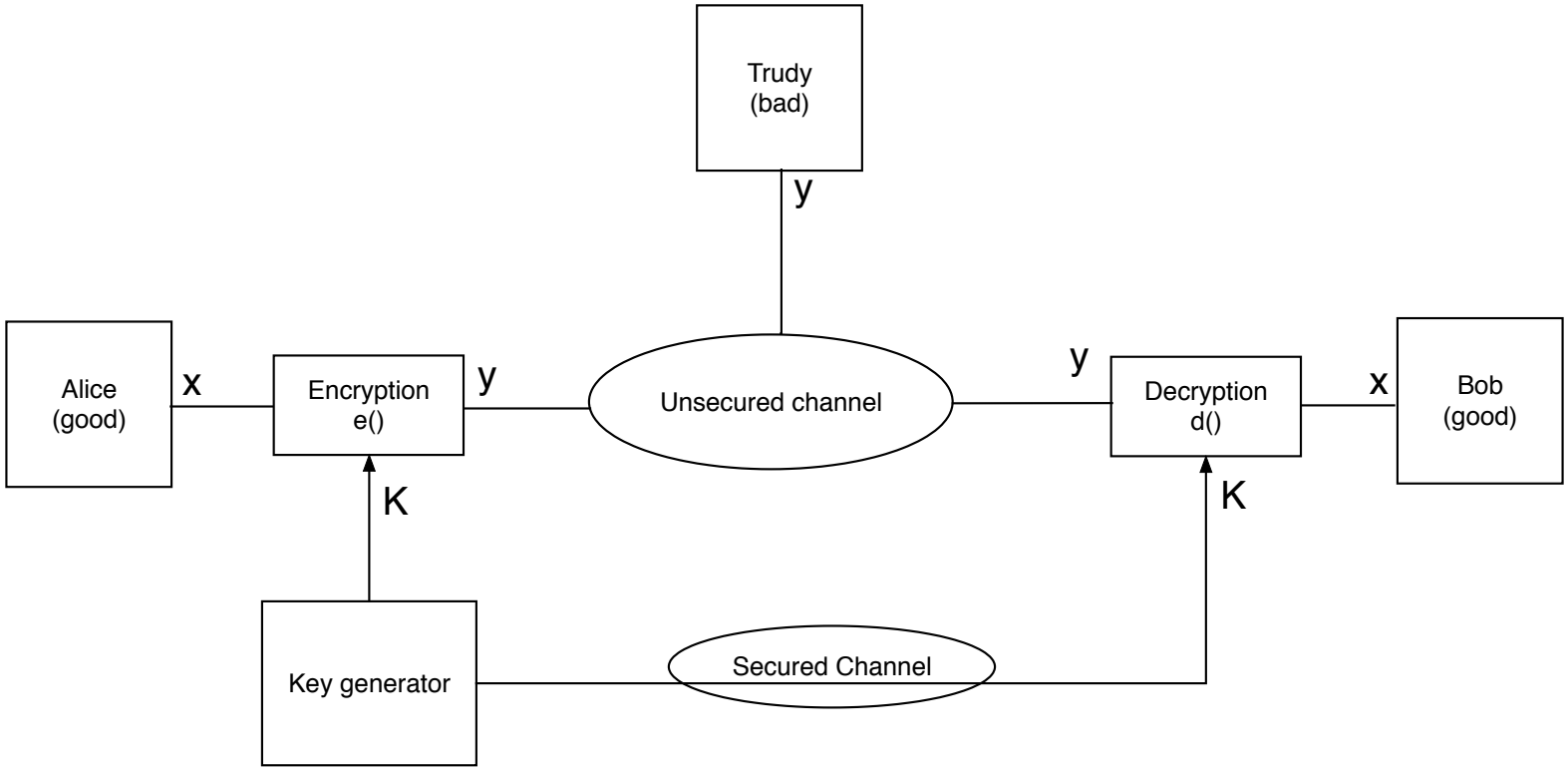
December 26, 2022

Session 2: Introduction to Cryptography - Symmetric Cryptography

Classification of the field of Cryptology



Basics of Symmetric Cryptology



- x is called the plaintext
- y is called the ciphertext
- K is called the key

- Encryption: $y = e_K(x)$
- Decryption: $x = d_K(y)$
- If same keys are used for encryption and decryption:
  $d_K(y) = d_K(e_K(x)) = x$

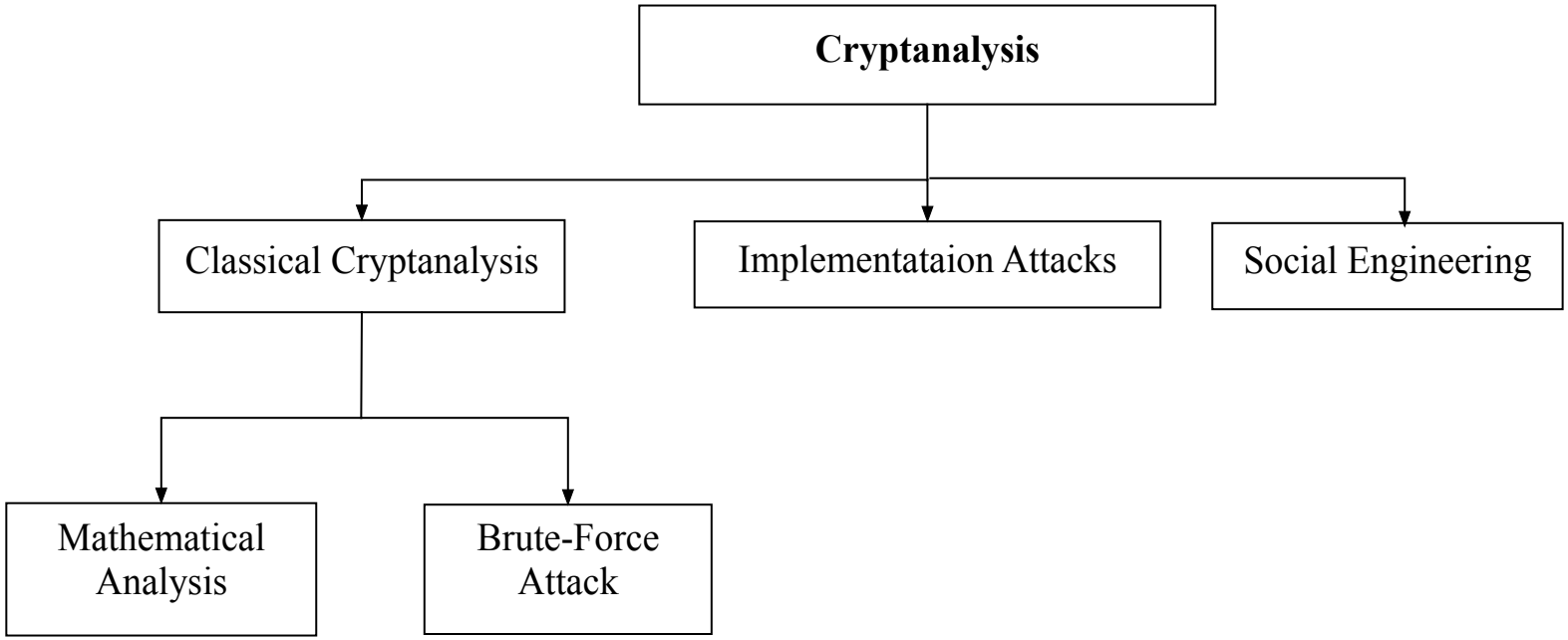
Cryptanalysis

- Why we need Cryptanalysis?
  The only way to assure a cipher is secure is to try and to break it (and fail!)

Kerchhoff's principle

A cryptosystem should be secure even if the attacker knows all details about the system, with the exception of the secret key. In particular, the system should be secure when the attacker knows the encryption and decryption algorithms.

Cryptanalysis Classification



- **Classical Cryptanalysis** : recovering x or k from y
- **Implementation Attacks** : try to extract a secret key from side-channel analysis, e.g., power measurement, electromagnetic radiation, etc.
- **Social engineering** : obtain a secret key by involving humans, e.g., trick a user into giving her password

Brute-Force Attack (Exhaustive Key Search) against Symmetric Ciphers

- Requires at least 1 plaintext-ciphertext pair (x_0, y_0)
- Check all possible keys K until: $d_K(y_0) = x_0$
- How many keys do we need?

Key length	Key space	Time for all keys searching
64 bits	2^{64}	few hours or days
128 bits	2^{128}	decades without quantum computer
256 bits	2^{256}	decades with quantum computer

Substitution cipher

- Historical cipher
- Example for understanding Brute-force and analytical attacks
- Encrypts letter rather than bits

Example

Idea: replace each plaintext letter by a fixed other letter.

Plaintext		Ciphertext
A	→	k
B	→	d
C	→	w
	....	

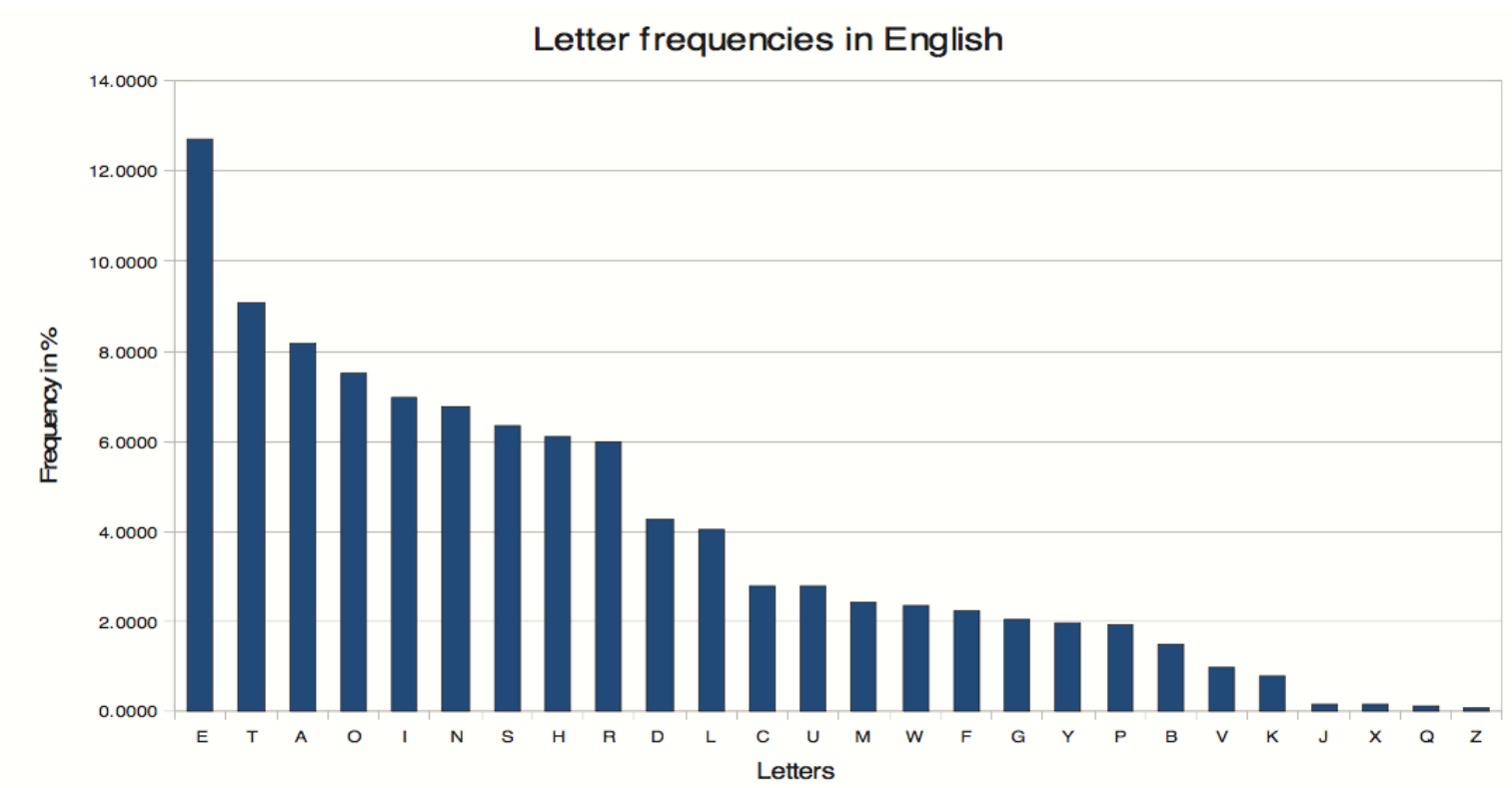
- Ciphertext:

```
iq ifcc vqqr fb rdq vfllcq na rdq cfjwhwz hr bnnb  hcc
                hwwhbsqvqbre hwq vhlq
```

- Brute-forte Attack?
- Analytical attack?

Example

- Brute-forte attack: 2^{40} per seconds $->$ How much time to break the code?
- Analytical: frequency counts



Historical cipher system

1. Shift (Ceasar) Cipher
2. Affine Cipher

Shift (Ceasar) Cipher - Example

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

- plaintext = ictlab
- ciphertext = lfwode
- What is the rule?

Shift Cipher - Description

Let $k,\ x,\ y \in 0, 1, ..., 25$

- Encryption: $y = e_k(x) \equiv (x + k) \mod 26$
- Decryption: $x = d_k(x) \equiv (y - k) \mod 26$

Question:

- Keyspace = ?
- Is it secure? (Any attack is possible?)

Affine Cipher

A key is consisted of two parts: $k = (a, b)$
Let $k,\ x,\ y \in 0, 1, ..., 25$

- Encryption: $y = e_k(x) \equiv (a.x + b) \mod 26$
- Decryption: $x = d_k(x) \equiv (a^{-1}.(y - b)) \mod 26$
- gcd(a,26)=1, then $a = \{1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25\}$

Keyspace =? Is it secure?