MSA
UNIVERSITY
IN EGYPT SINCE 1996
Established by Dr.Nawal El Degwi
MSA UNIVERSITY
جامعة أكتوبر للعلوم الحديثة والآداب
The First British Higher Education in Egypt

Cryptography ECE5632 - Spring 2026

Lecture 1B

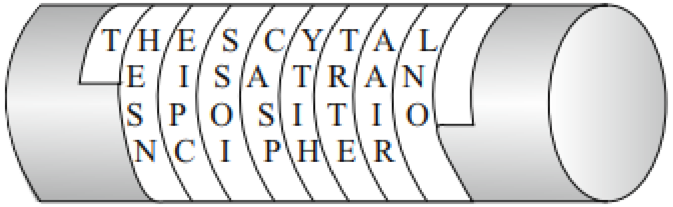
Dr. Farah Raad

Lecture Topic

Introduction

Cryptography

- ➢ First associations might be e-mail encryption, secure website access, smart cards for banking applications or code-breaking during World War II (famous attack against the German Enigma encryption machine).
- ➢ Seems closely linked to modern electronic communication. However, cryptography is a rather old business back to about 2000 B.C., “secret” hieroglyphics were used in ancient Egypt.
- ➢ Has been used in many cultures that developed written language,(Letter-based encryption schemes) secret writing in ancient Greece, namely the **Scytale of Sparta**, or the famous **Caesar Cipher** in ancient Rome.

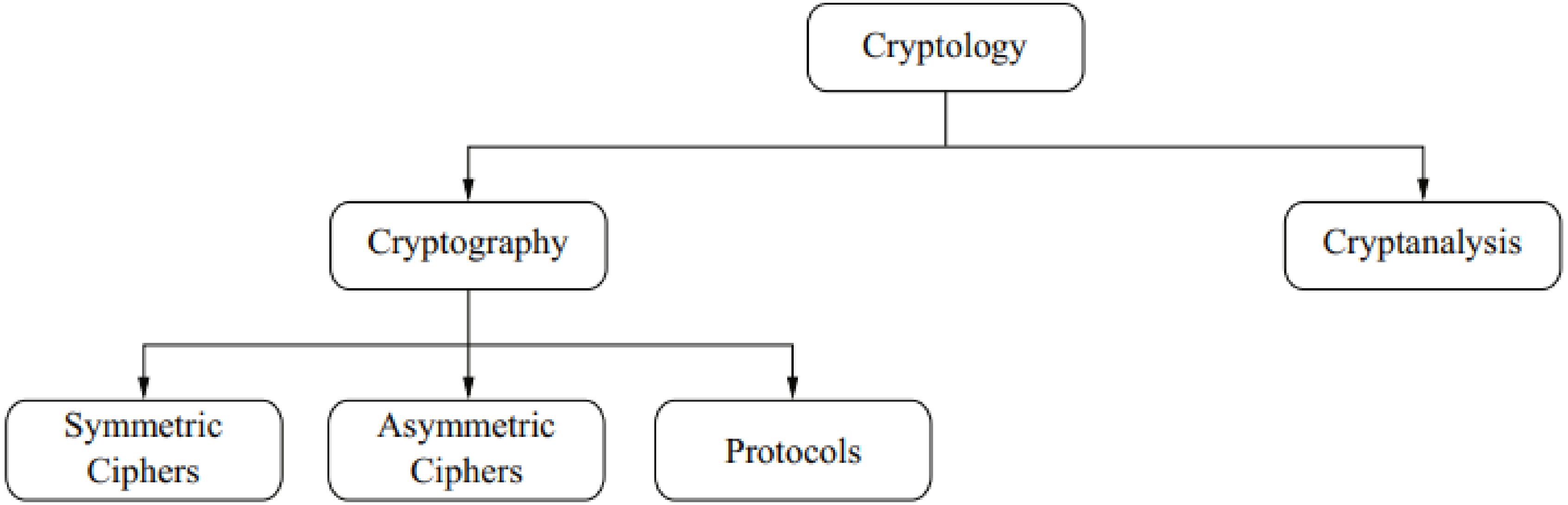


Scytale of Sparta

German Enigma encryption machine

Classification of the Field of Cryptology

- The most general term is cryptology and not cryptography.
- Cryptography is the science of secret writing with the goal of hiding the meaning of a message.
- Cryptanalysis is the science and sometimes art of breaking cryptosystems.
- Because cryptanalysis is the only way to assure that a cryptosystem is secure, it is an integral part of cryptology.



Classification of the Field of Cryptology

Symmetric Algorithms (ciphers)

- Are two parties, encryption and decryption methods for which they share a secret key.
- Widely used since ancient times until 1976.
- Symmetric ciphers are still in widespread use, especially for data encryption and integrity check of messages.

Asymmetric (or Public-Key) Algorithms (ciphers)

- In 1976 an entirely different type of cipher was introduced by Whitfield Diffie, Martin Hellman and Ralph Merkle.
- In public-key cryptography, a user possesses a secret key as in symmetric cryptography but also a public key.
- can be used for applications such as digital signatures and key establishment, and also for classical data encryption.

Hybrid Schemes: The majority of today‘s protocols are hybrid schemes, i.e., the use both

- Symmteric ciphers (e.g., for encryption and message authentication)
- Asymmetric ciphers (e.g., for key exchange and digital signature).

Classification of the Field of Cryptology

- **Cryptographic Protocols Roughly speaking**, crypto protocols deal with the application of cryptographic algorithms.

- Symmetric and asymmetric algorithms can be viewed as building blocks with which applications such as secure Internet communication can be realized.

- The Transport Layer Security (TLS) scheme, which is used in every Web browser, is an example of a cryptographic protocol.

- In the majority of cryptographic applications in practical systems, symmetric and asymmetric algorithms (and often also hash functions) are all used together (hybrid schemes).

- The reason for using both families of algorithms is that each has specific strengths and weaknesses.

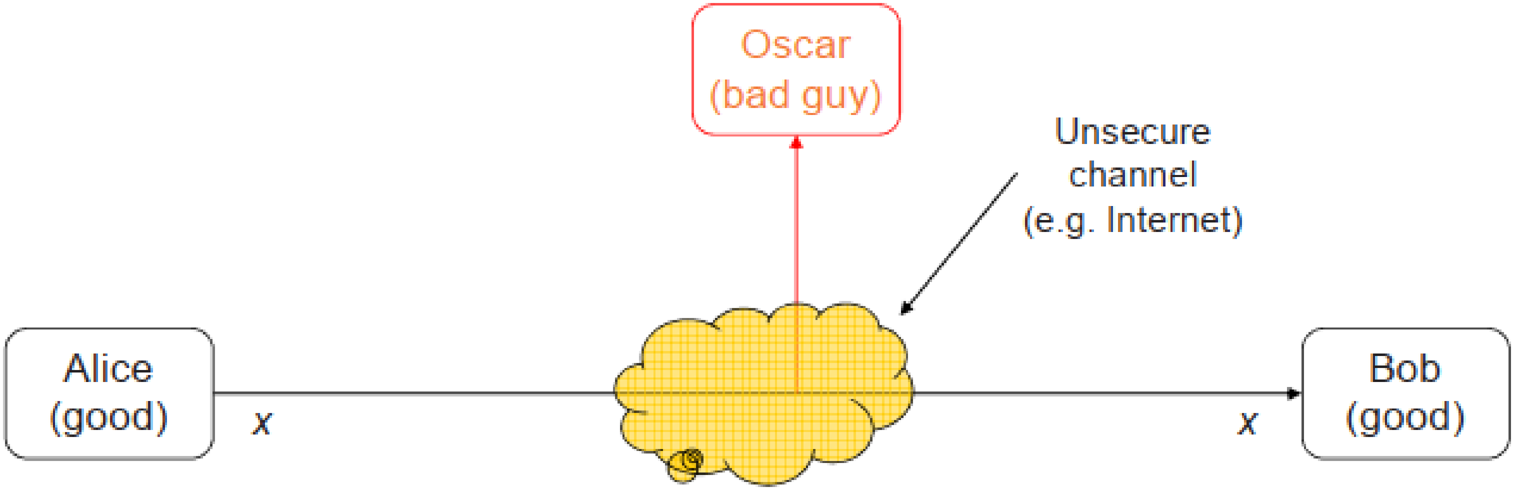
Symmetric Cryptography

- Alternative names: **private-key**, **single-key** or **secret-key** cryptography

Problem Statement:

1) Alice and Bob would like to communicate via an unsecure channel (e.g., WLAN or Internet).
2) A third party Oscar (the bad guy) has channel access but should not be able to understand the communication.

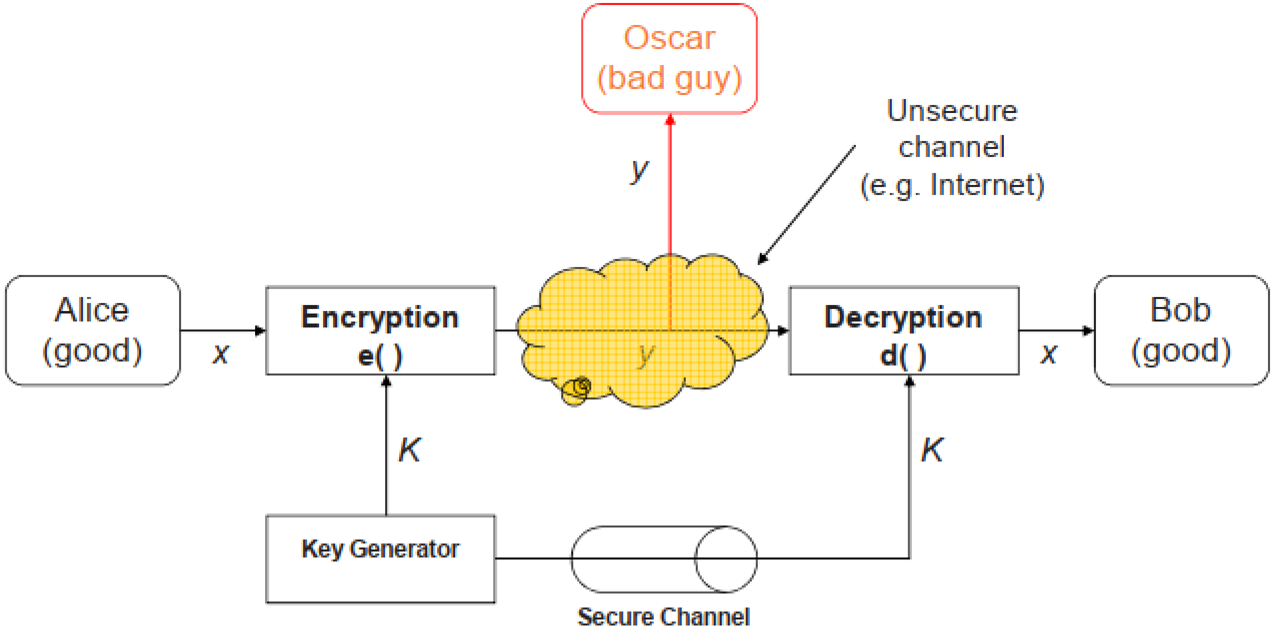
This type of unauthorized listening is called eavesdropping.



Symmetric Cryptography

Solution:

Encryption with symmetric cipher.
Oscar obtains only ciphertext y, that looks like random bits.



- x is the. **Plaintext** or *cleartext*
- y is the **ciphertext**
- *K* is the **key**
- Set of all keys {*K*1, *K*2, ...,*Kn*} is the **key space**

Symmetric Cryptography

- Encryption equation $\mathbf{y = e_K(x)}$
- Decryption equation $\mathbf{x = d_K(y)}$

Encryption and decryption are inverse operations if the same key K is used on both sides:

$$d_K(y) = d_K(e_K(x)) = x$$

<u>Important:</u> The key must be transmitted via a **secure channel** between Alice (Transmitter) and Bob (Receiver).

- The secure channel can be realized, e.g., by manually installing the key for the Wi-Fi Protected Access (WPA) protocol or a human courier.
- However, the system is only secure if an attacker does not learn the key K!

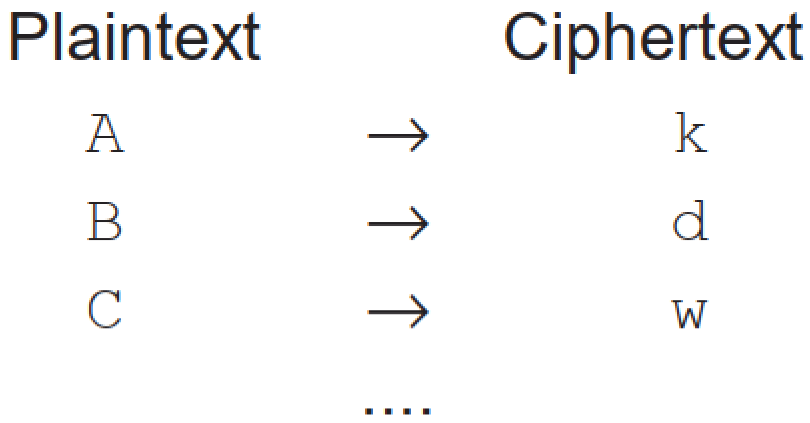
⇒ The problem of secure communication is reduced to secure transmission and storage of the key K

Simple Symmetric Encryption:

➢ The Substitution Cipher

- It is one of the simplest methods for encrypting text, the substitution (= replacement) cipher.
- Historical cipher
- Encrypts letters rather than bits (like all ciphers until after WW II)
- We will use the substitution cipher for learning some important facts about key lengths and about different ways of attacking ciphers (brute-force vs. analytical attacks).

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



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

For instance, the pop group **ABBA** would be encrypted as **kddk.**

- Substitution table is chosen completely randomly so that an attacker is not able to guess it.
- The substitution table is the key of this cryptosystem.

Cryptanalysis

What do you think about Breaking Cryptosystems ??

Cryptanalysis

➢ Why do we need Cryptanalysis?

- There is no *mathematical proof of security* for any practical cipher
- The only way to have assurance that a cipher is secure is to try to break it (and fail) !

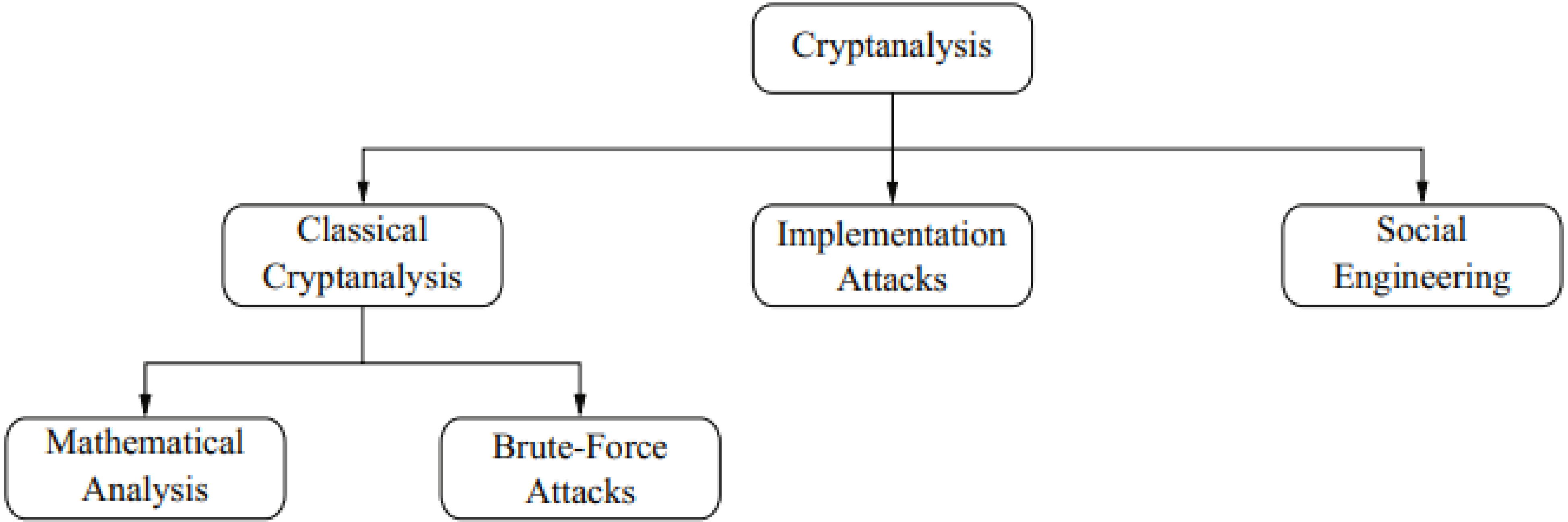
Kerckhoffs’ Principle

- *A cryptosystem should be secure even if the attacker knows all details about the system, with the exception of the secret key.*

Security by Obscurity.

In order to achieve Kerckhoff‘s Principle in practice:
Only use widely known ciphers that have been cryptanalyzed for several years by good cryptographers! (*Understanding Cryptography* only treats such ciphers)

Classification of Cryptanalysis



1. Classical Cryptanalysis

➢ Brute-Force Attack

- which treat the encryption algorithm as a black box and test all possible keys

➢ Mathematical Analysis

- which exploit the internal structure of the encryption method

❖ It is understood as the science of recovering the plaintext x from the ciphertext y, or, alternatively, recovering the key k from the ciphertext y.

2. Implementation Attacks

- It can be used to obtain a secret key, by measuring the electrical power consumption of a processor which operates on the secret key. by applying signal processing techniques.

- Also, electromagnetic radiation or the runtime behavior of algorithms can give information about the secret key.

- Note also that implementation attacks are mostly relevant against cryptosystems to which an attacker has physical access, such as smart cards.

- In most Internet-based attacks against remote systems, implementation attacks are usually not a concern.

3. Social Engineering Attacks

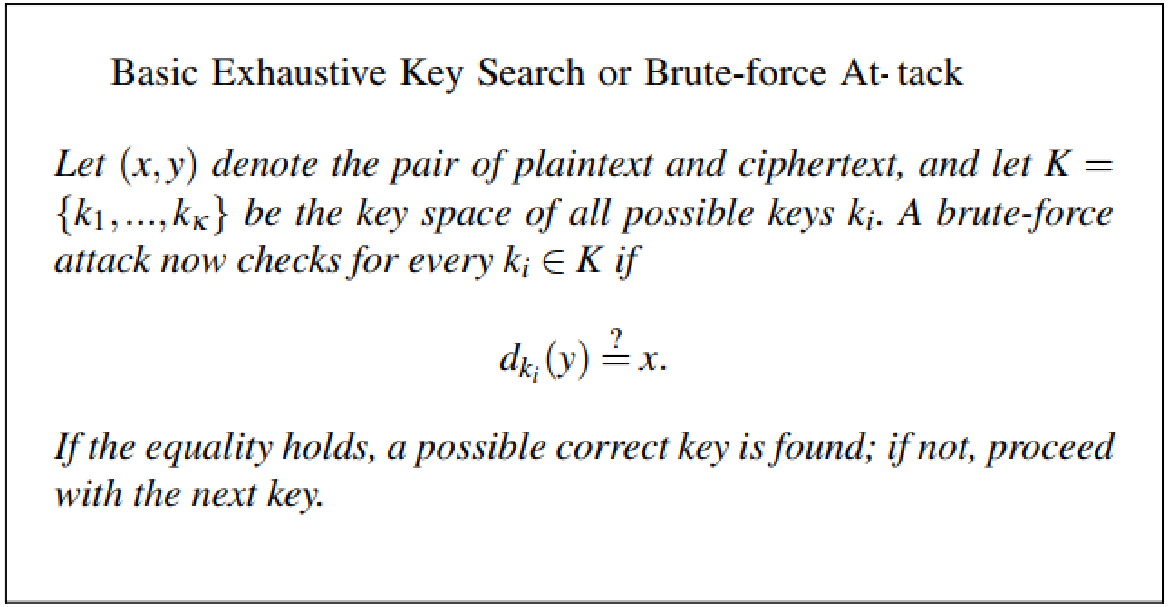
E.g., trick a user into giving up her password

Ways of breaking the cipher

Attacks against the Substitution Cipher

First Attack: Exhaustive Key Search (Brute-Force Attack)

- Treats the cipher as a black box
- Requires (at least) 1 plaintext-ciphertext pair (x0, y0)
- Check all possible keys until condition is fulfilled.



Basic Exhaustive Key Search or Brute-force At- tack

Let (x,y) *denote the pair of plaintext and ciphertext, and let* $K = \{k_1,\ldots,k_\kappa\}$ *be the key space of all possible keys* k_i*. A brute-force attack now checks for every* $k_i \in K$ *if*

$$d_{k_i}(y) \stackrel{?}{=} x.$$

If the equality holds, a possible correct key is found; if not, proceed with the next key.

Based on a simple concept:

The attacker has the ciphertext from eavesdropping on the channel and happens to have a short piece of plaintext. e.g., the header of a file that was encrypted.

✓ In practice, a brute-force attack can be more complicated because incorrect keys can give false positive results.

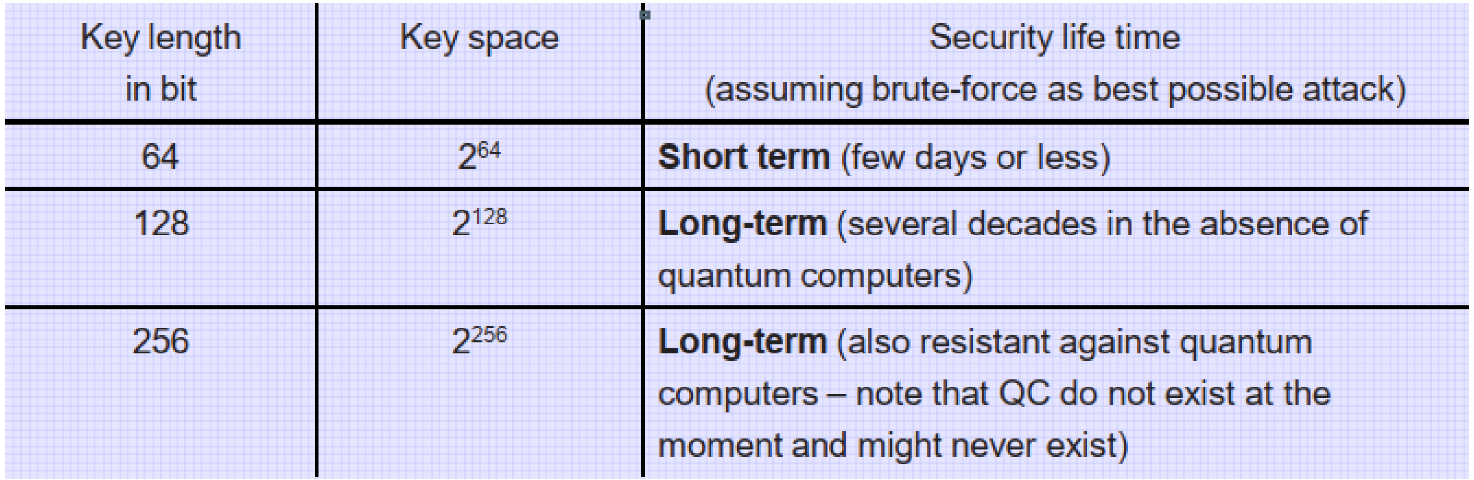
How can determine the key space of the substitution cipher ?

When choosing the replacement for the first letter A, we randomly choose one letter from the 26 letters of the alphabet. The replacement for the next alphabet letter B was randomly chosen from the remaining 25 letters, etc.

Thus there exist the following number of different substitution tables:

$$\text{key space of the substitution cipher} = 26 \cdot 25 \cdots 3 \cdot 2 \cdot 1 = 26! \approx 2^{88}$$

- ❖ Search through 2^{88} keys is completely infeasible with personal computers!



Key length in bit	Key space	Security life time (assuming brute-force as best possible attack)
64	2^{64}	**Short term** (few days or less)
128	2^{128}	**Long-term** (several decades in the absence of quantum computers)
256	2^{256}	**Long-term** (also resistant against quantum computers – note that QC do not exist at the moment and might never exist)

Important: An adversary only needs to succeed with **one** attack. Thus, a long key space does not help if other attacks (e.g., social engineering) are possible..

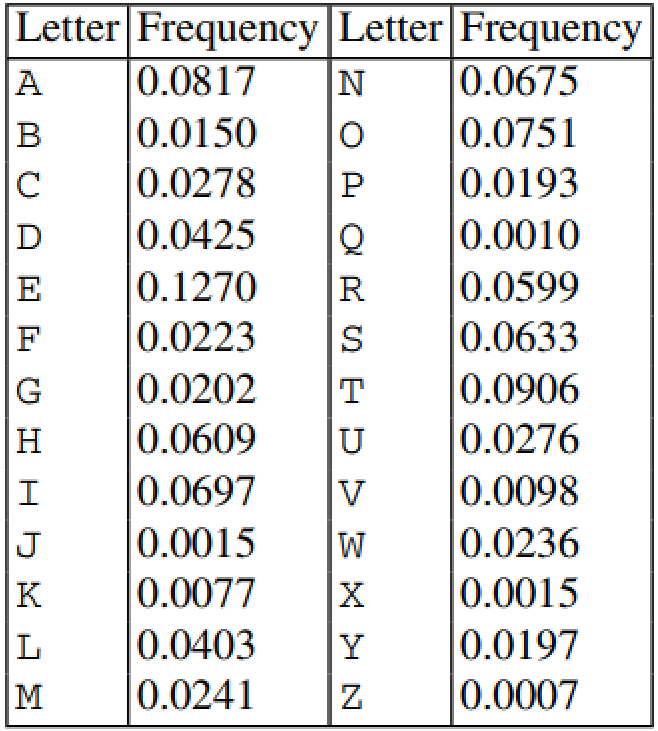
Attacks against the Substitution Cipher

Second Attack: Letter Frequency Analysis

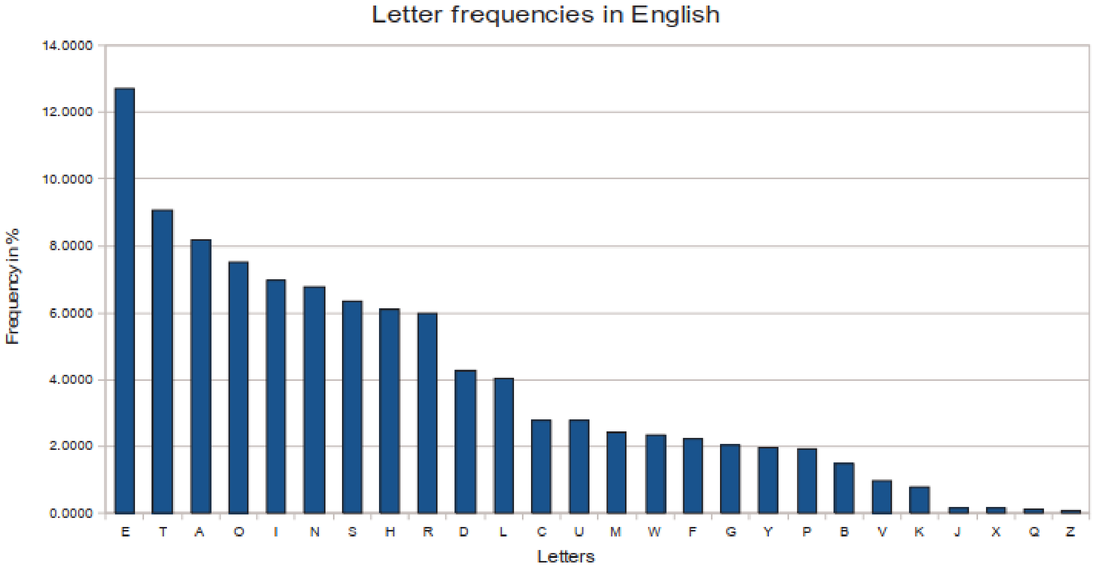
1. Determine the frequency of every ciphertext letter.
2. Looking at pairs or triples, or quadruples, and so on of ciphertext symbols. (the letter Q is almost always followed by a U).
3. If word separators (blanks) have been found (which is only sometimes the case), one can often detect frequent short words such as THE, AND, etc.

❖ Moreover: the frequency of plaintext letters is preserved in the ciphertext.

Table 1.1 Relative letter frequencies of the English language



Letter	Frequency	Letter	Frequency
A	0.0817	N	0.0675
B	0.0150	O	0.0751
C	0.0278	P	0.0193
D	0.0425	Q	0.0010
E	0.1270	R	0.0599
F	0.0223	S	0.0633
G	0.0202	T	0.0906
H	0.0609	U	0.0276
I	0.0697	V	0.0098
J	0.0015	W	0.0236
K	0.0077	X	0.0015
L	0.0403	Y	0.0197
M	0.0241	Z	0.0007



Example

- Let‘s retun to our example and identify the most frequent letter:

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

- We replace the ciphertext letter q by E and obtain:

iE ifcc vEEr fb rdE vfllcE na rdE cfjwhwz hr bnnb hcc hwwhbsEvEbre hwE vhlE

- By further guessing based on the frequency of the remaining letters we obtain the plaintext:

WE WILL MEET IN THE MIDDLE OF THE LIBRARY AT NOON ALL ARRANGEMENTS ARE MADE

Important lesson

Even though the substitution cipher has a sufficiently large key space of approximate 2^{88} *, it can easily be defeated with analytical methods. This is an excellent example that an encryption scheme must withstand all types of attacks.*

MSA UNIVERSITY
IN EGYPT SINCE 1996
Established by Dr.Nawal El Degwi
MSA UNIVERSITY
جامعة أكتوبر للعلوم الحديثة والآداب

Thank You!

See You next Lectures!!

Any Question?