187 - Day 1

Sunday, April 1, 2018 8:53 PM

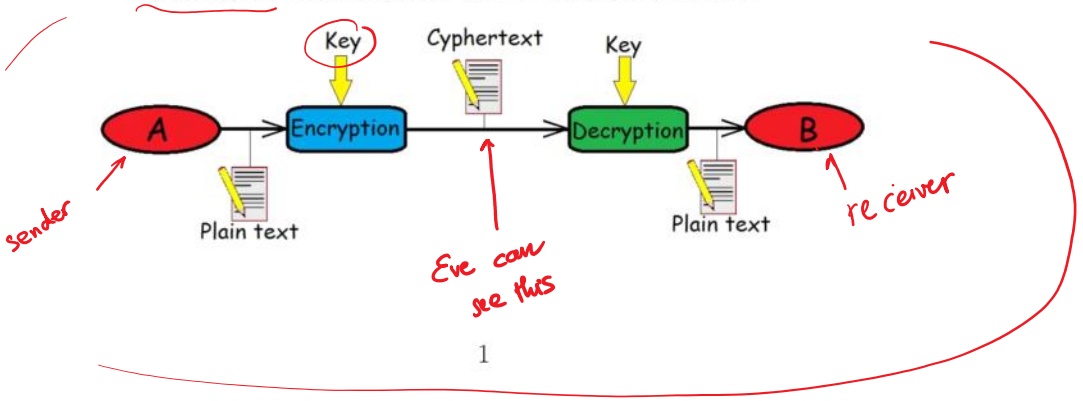
Day 01 –Introduction to Cryptography

Basic jargons of cryptography

- **Cryptography** is the study of methods of sending messages in disguised form so that only the intended recipients can remove the disguise and read the message.

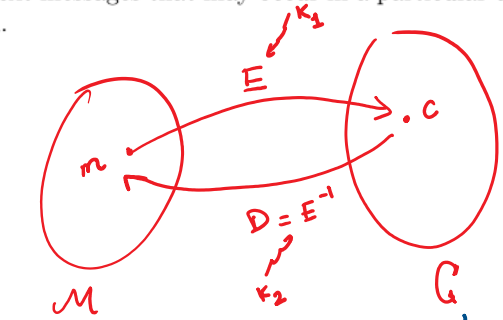
$$\begin{aligned} \textit{Cryptography} &= \textit{kryptos}\ (\kappa\rho\upsilon\pi\tau o\sigma) + \textit{graphen}\ (\gamma\rho\alpha\varphi\eta\nu) \\ &= \text{“}\textit{hidden/secret}\text{”} + \text{“}\textit{writing}\text{”} \end{aligned}$$

- **Plaintext:** the message *before* it has been encrypted.
- **Ciphertext:** the message *after* it has been encrypted.
- **Encryption/enciphering:** the act of hiding the plaintext by transforming it into an undecipherable code. Encryption typically uses a specified parameter or **key** to perform the data transformation.
- **Decryption/deciphering:** the opposite of encryption. Decryption of encrypted data recovers the original data.
- The **sender** and **receiver** who want to communicate in secret are usually called **Alice** and **Bob**.
- The **opponent** who tries to intercept Alice and Bob's message usually is called **Eve**.
- A **cipher/cypher** is a method of secret writing.
- **Cryptosystem** encompasses all the components above:



Ex: 2-grams: XO, AC, SX, ...
3-grams: THE, AAB, ...

- An **n-gram** is a string of n letters.
- A **key** is usually a sequence of digits or symbols that is used to determine the algorithm by which plaintext is to be transformed into ciphertext. A key that is used only once is called a one-time pad/key.
- The **key space** (usually denoted as $\mathcal{K}$) is the collection of all keys that may occur in a given cryptosystem.
- The **message/plaintext space** (usually denoted as $\mathcal{M}$) is the collection of all plaintext messages that may occur in a particular cryptographic transaction.
- The **ciphertext space** (usually denoted as $\mathcal{C}$) is the collection of all plaintext messages that may occur in a particular cryptographic transaction.



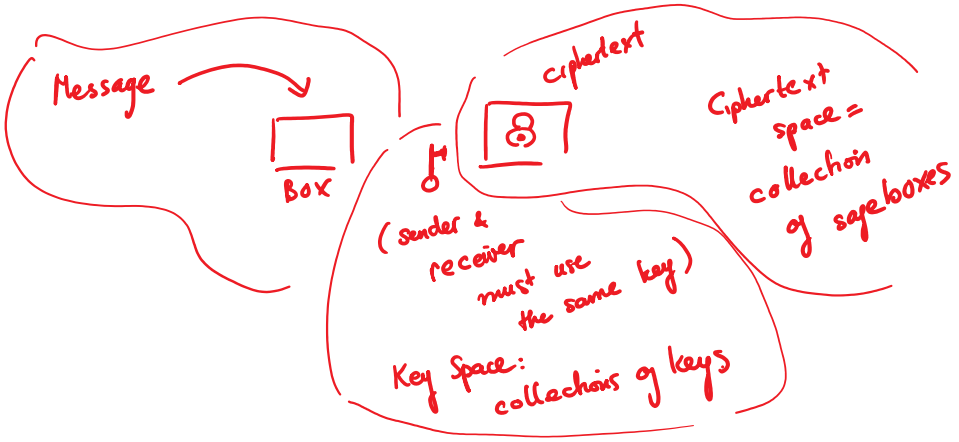
Note: K_1 & K_2 may be different.

Methods of encryption

There are two basic method of encryptions

- **Substitution:** individual letters or n-grams of plaintext are **replaced** by letters or n-grams of ciphertext.
- **Transposition:** the characters or words of the original message are **rearranged** according to some particular patterns.

Most known modern methods are a mixture of both.



hieroglyphs : ancient Egyptian writing

word → picture.

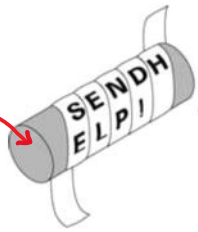
subs.

Some examples

Rosetta Stone : found in 17--

Fully decryted by Jean-François Champollion in 1822

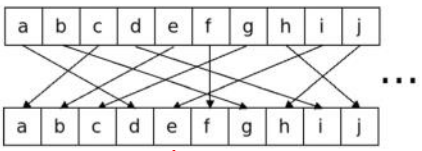
key



scytale (used by Spartans) ~ 400 BCE

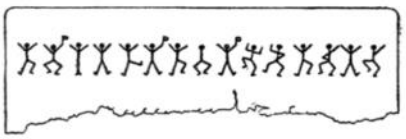
transposition

Need an identical rod to decrypt



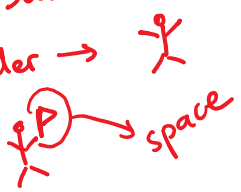
generalized mono-alphabetic subs.

(more on Wednesday)



Dancing man subs.

letter →

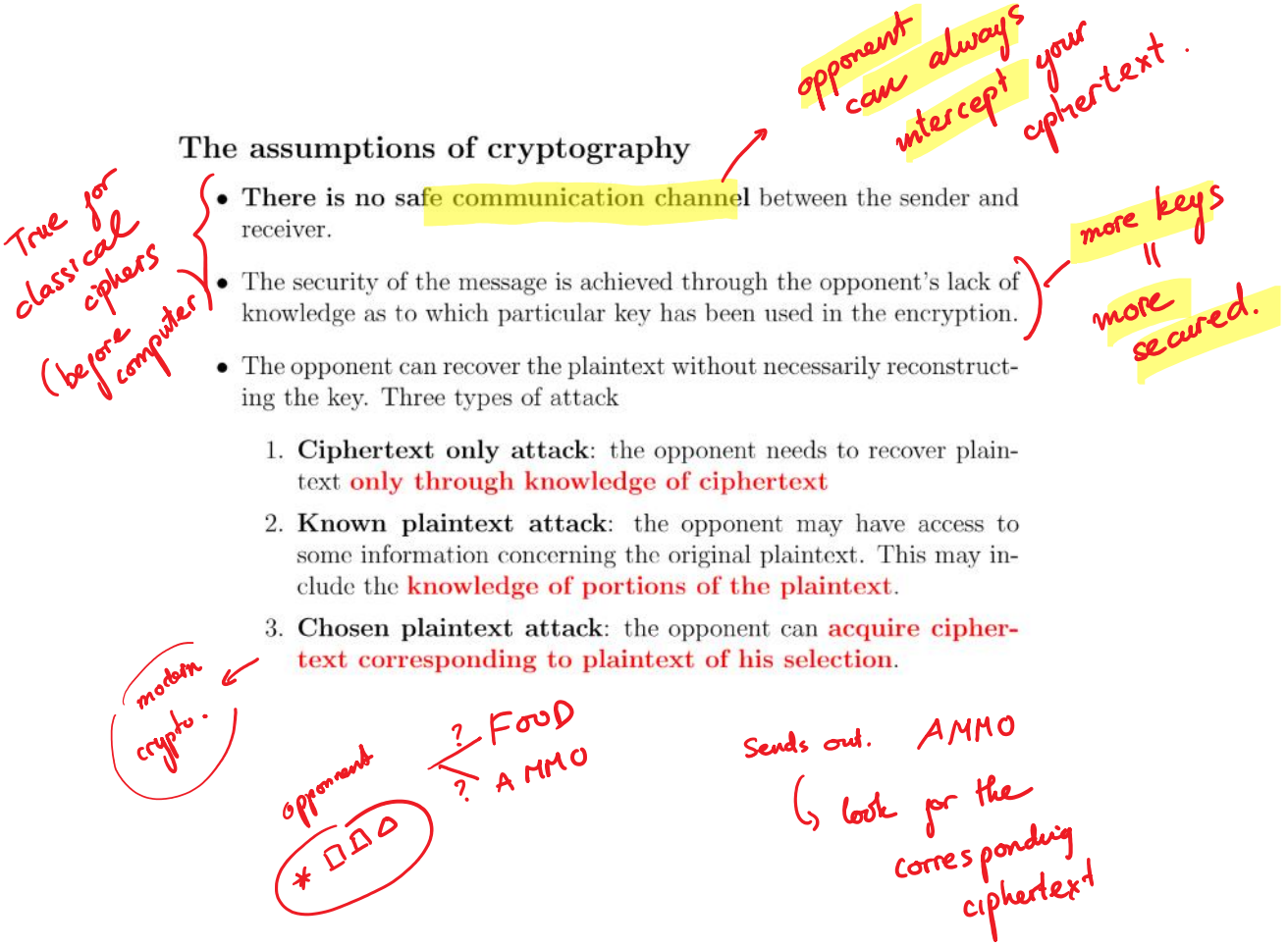


space

The assumptions of cryptography

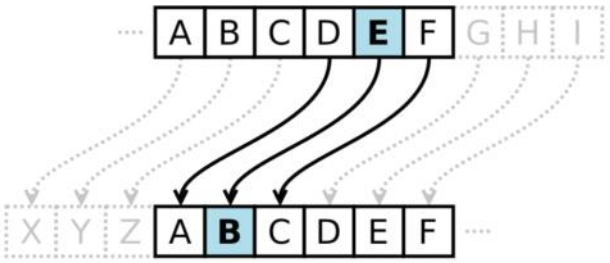
- **There is no safe communication channel** between the sender and receiver.
- The security of the message is achieved through the opponent's lack of knowledge as to which particular key has been used in the encryption.
- The opponent can recover the plaintext without necessarily reconstructing the key. Three types of attack

  1. **Ciphertext only attack**: the opponent needs to recover plaintext **only through knowledge of ciphertext**
  2. **Known plaintext attack**: the opponent may have access to some information concerning the original plaintext. This may include the **knowledge of portions of the plaintext**.
  3. **Chosen plaintext attack**: the opponent can **acquire ciphertext corresponding to plaintext of his selection**.



The Caesar cipher

- Invented by Julius Caesar 2,000 years ago.
- This is a **substitution cipher** in which each letter in the plaintext is replaced by a letter some *fixed* number of positions down the alphabet



plaintext → ciphertext

E → B

G → D

⋮

keep the same order of the alphabet.

Q-shift

A	B	C	D	E	F	G	H	I	J	K	L	M	N
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D

O	P	Q	R	S	T	U	V	W	X	Y	Z
E	F	G	H	I	J	K	L	M	N	O	P

plaintext → STARZ → I J Q H P → ciphertext.

$|K|$ = # keys = # letters in the alphabet

= 26 for English.

or 25 if we don't count the identical map A → A

Can be broken easily - just exhaust all 26 possibilities!

Shift	*Candidate plaintext*
A	*exxegoexsrgi*
B	*dwwdfndwrqfh*
C	*cvvcemcvqpeg*
D	*buubdlbupodf*
E	*attackatonce*
F	*zsszbjzsnmbd*
...	...
X	*haahjrhavujl*
Y	*gzzgiqgzutik*
Z	*fyyfhpfytshj*

ciphertext.

plaintext