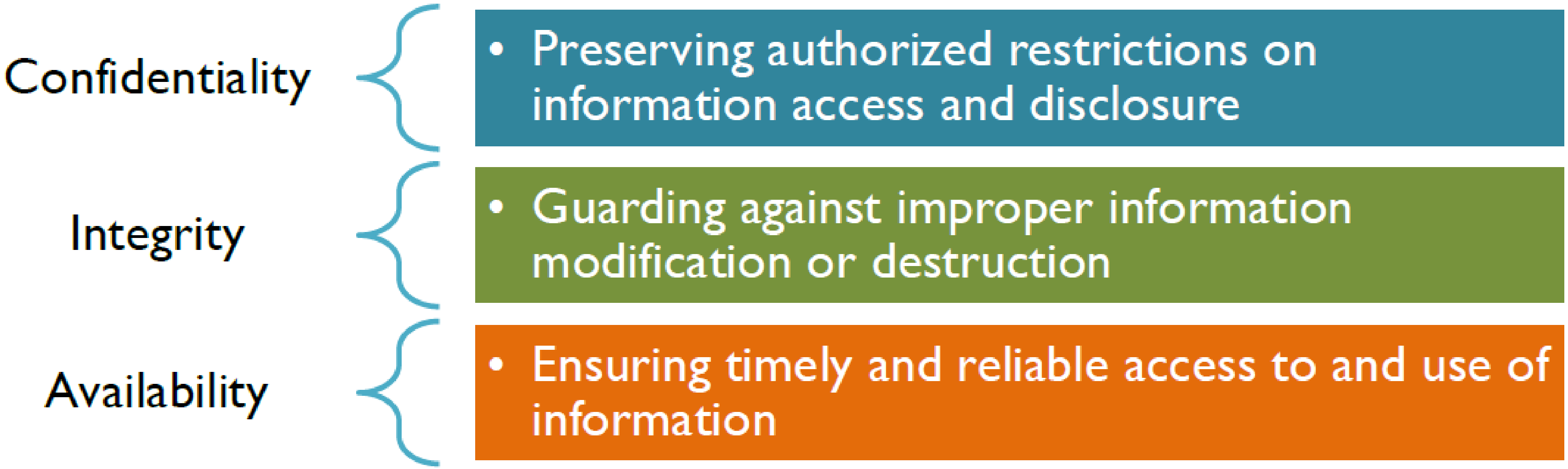
Basic Principles

Harshan Jagadeesh
Department of Electrical Engineering,
IIT Delhi

References and notes used from:

Cryptography and Network Security, Principles and Practices, by William Stallings (combination of several editions)

Cryptography and network security course at SCSE, NTU by Prof. Anwitaman Datta



Confidentiality

- Preserving authorized restrictions on information access and disclosure

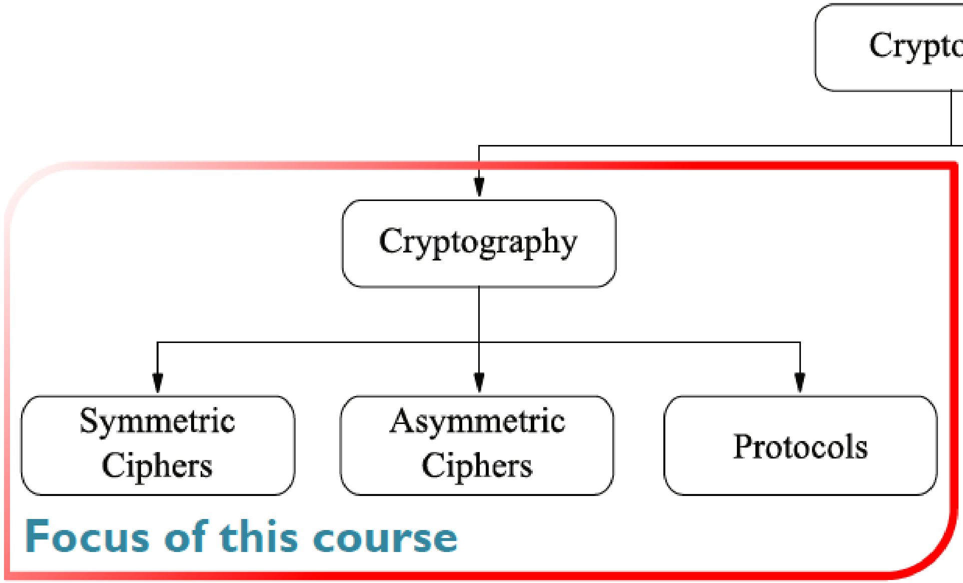
Integrity

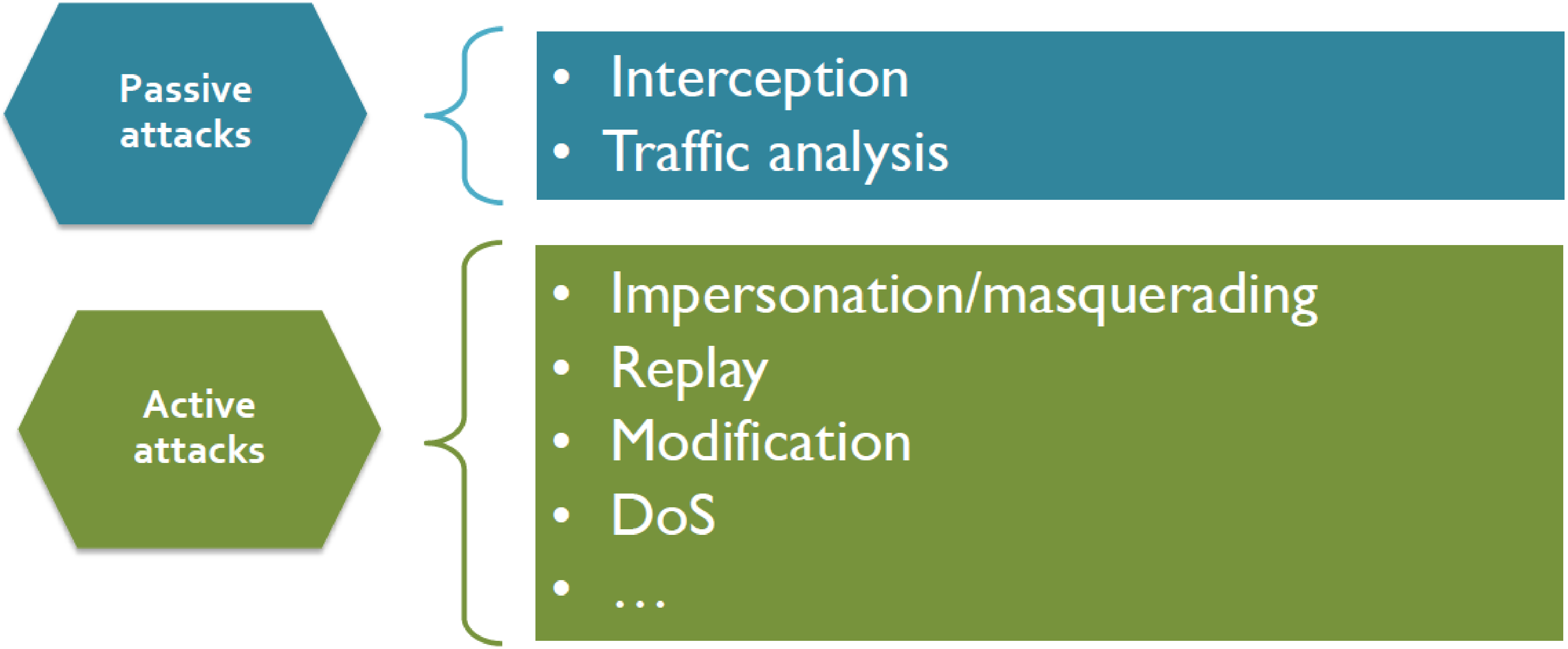
- Guarding against improper information modification or destruction

Availability

- Ensuring timely and reliable access to and use of information

⌘ Many aspects to realizing a proper security solution: cryptology is just one (but very *important and necessary*) part





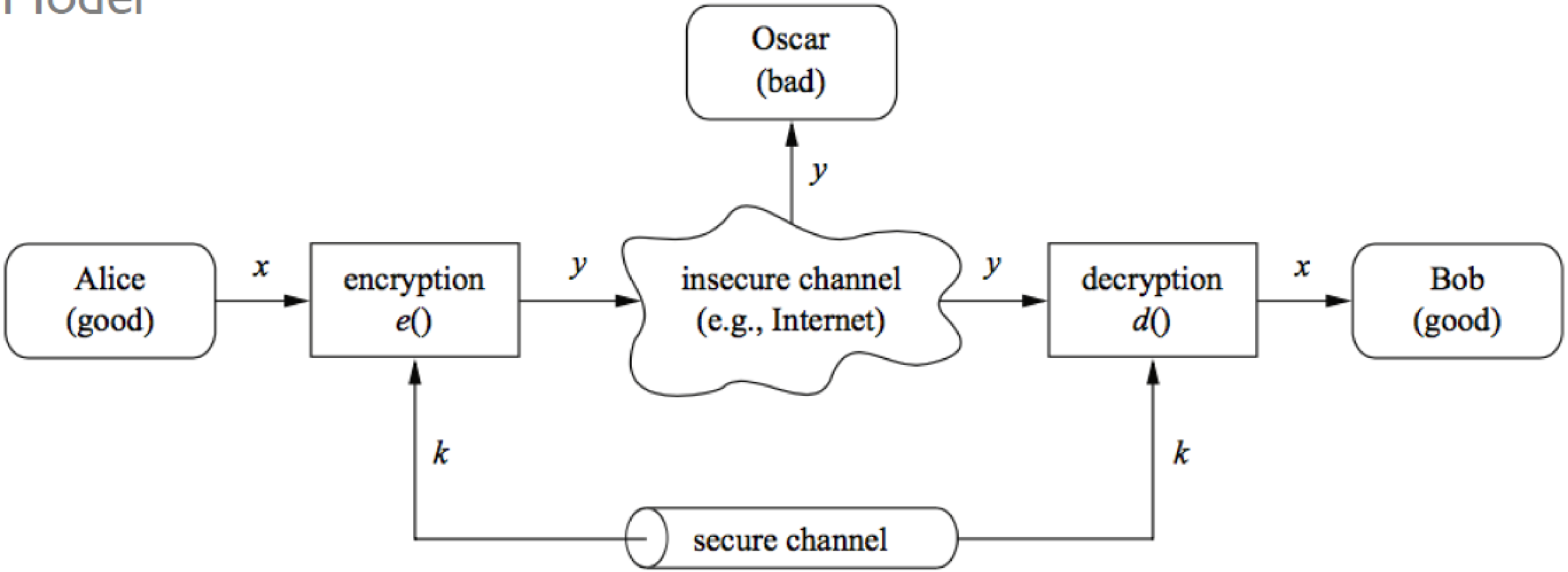
Passive attacks

- Interception
- Traffic analysis

Active attacks

- Impersonation/masquerading
- Replay
- Modification
- DoS
- …

Model



⌘ **Sender/Receiver** share a common secret key ***k***

- Encryption & Decryption both done with same key (hence, symmetric)

YMNX HTZWXJ BNQQ GJ KZS

- One of the simplest form of substitution cipher: **k-shift cipher**
  - consider the following numerical equivalent assignment to each letter:

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

- The **k-shift cipher** uses the mappings:

Encryption: $C = E(k,p) = (p+k) \ \textbf{mod}\ 26$

Decryption: $p = D(k,C) = (C-k) \ \textbf{mod}\ 26$

LEGEND

p	plain text
C	cipher text
k	secret key
E()	encryption algorithm
D()	decryption algorithm

- Given that the above ciphertext (title) uses a k-shift cipher
  decipher it without knowing the key

Since the "algorithm" is known, a brute-force attack* (exhaustive search for the "key"), i.e., checking 25 possibilities, in this case, would suffice. If one is lucky, the search can be terminated much earlier.

* Trivia: The term brute-force search has nothing to do with "Et tu, Brutus!", but a 3-shift cipher was used by Caesar (and the algorithm was not supposedly known to the adversaries). This specific instance (3-shift) cipher is thus known as **Caesar cipher**.

Kerckhoff’s principle

⌘ A cryptosystem should be secure even if the attacker (Oscar) knows all details about the system, with the exception of the secret key.

In particular, the system should be secure even when the attacker knows the encryption and decryption algorithms (but not the secret key).

Security solely by obscurity is vulnerable to reverse engineering.

Use of known algorithms aide commoditization of cryptography.

Auguste Kerckhoffs (1835-1903)
Dutch linguist & cryptographer

Monoalphabetic cipher

⌘ Each plaintext symbol is substituted with a unique ciphertext symbol

- the interpretation of symbol can be flexible: single letters, n-grams, …

k-shift cipher: Assignment of substituting symbols is in a sequence

e.g., Caesar cipher: D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

Only 25 possible encryptions, easy to brute-force!

If any random permutation is used as a cipher:

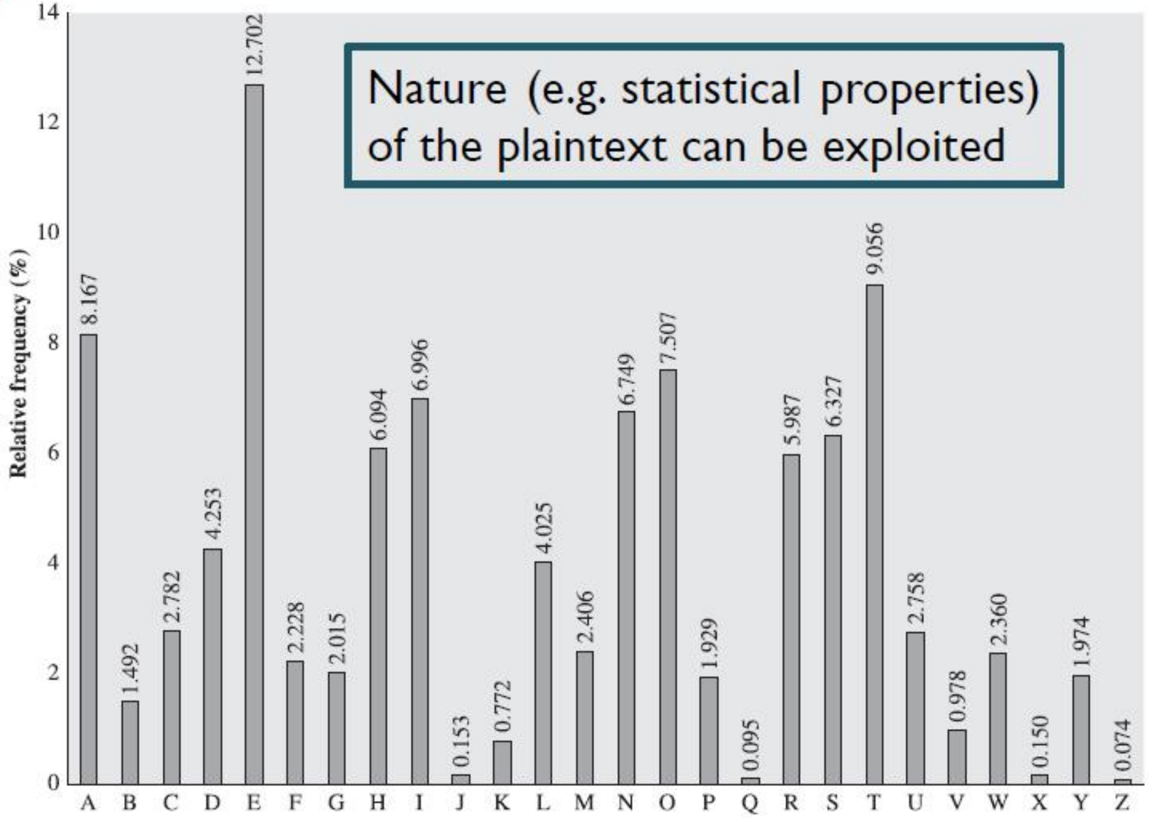
Fragment of a possible cipher: X H R O Q U L …

How many possibilities?

Not quite ಠ_ಠ

PROBLEM SOLVED!

- ⌘ Cryptanalysis instead of brute-force



Nature (e.g. statistical properties) of the plaintext can be exploited

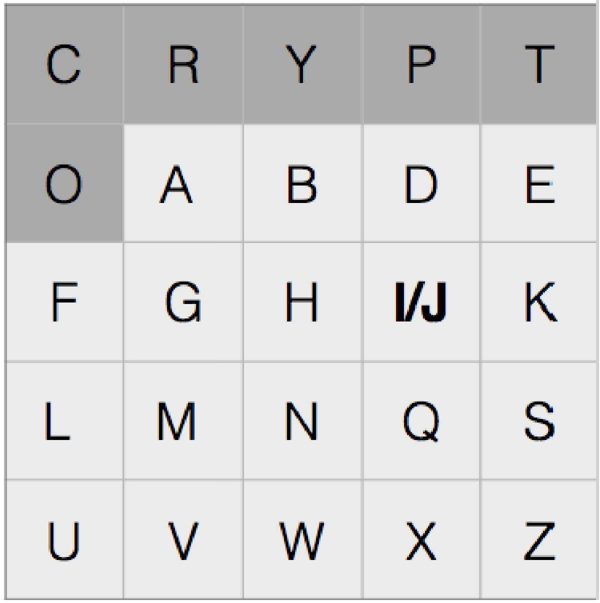
Playfair cipher

- Idea: multi-letter encryption to reduce structural information

e.g. aq → DM
av → GR
vq → XM

➡ Playfair cipher web demo

Note that these multi-letter n-grams (in fact, digrams) are each to be seen as single plaintext “symbol”, and Playfair is thus still a monoalphabetic cipher.



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

Playfair cipher: Initialization

- Select a (secret) *keyword*, say CRYPTOCRYO
- Populate a 5*5 matrix, left-to-right, top-to-bottom with the keyword (omit duplicate letters)
- Complete the matrix alphabetically with unused letters

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

I/J are considered as *equivalent*

Playfair cipher: Encryption

- If letters in a pair fall in same row, replace with letter on the right (warp)
- If letters in a pair fall in same column, replace with letter beneath (warp)
- Otherwise: Replace plaintext letter with letter in same row, but column of the paired letter

key: CRYPTOCRYO

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

Example:

Plaintext: cool dude
Encryption input: co ol du de
Ciphertext: OF FU OX EO

Different plain text letters were mapped to same ciphertext letter

Same mapping is still possible depending on coincidental co-occurrences

Polyalphabetic substitution

- A set of monoalphabetic ciphers used,
  choice of cipher in each step determined by a key

e.g., Vigenère cipher

plaintext:	$p_0, p_1, p_2, \cdots p_{n-1}$
keyword:	$k_0, k_1, k_2, \ldots k_{m-1}$
encryption:	$C_i = (p_i + k_{i \; mod \; m}) \; mod \, 26$
decryption:	$p_i = (C_i - k_{i \; mod \; m}) \; mod \, 26$

Transposition technique

- A slightly more sophisticated technique

Plaintext:	a	t	t	a	c	k	p
	o	s	t	p	o	n	e
	d	u	n	t	i	l	t
	w	o	a	m	x	y	z

Transposition technique

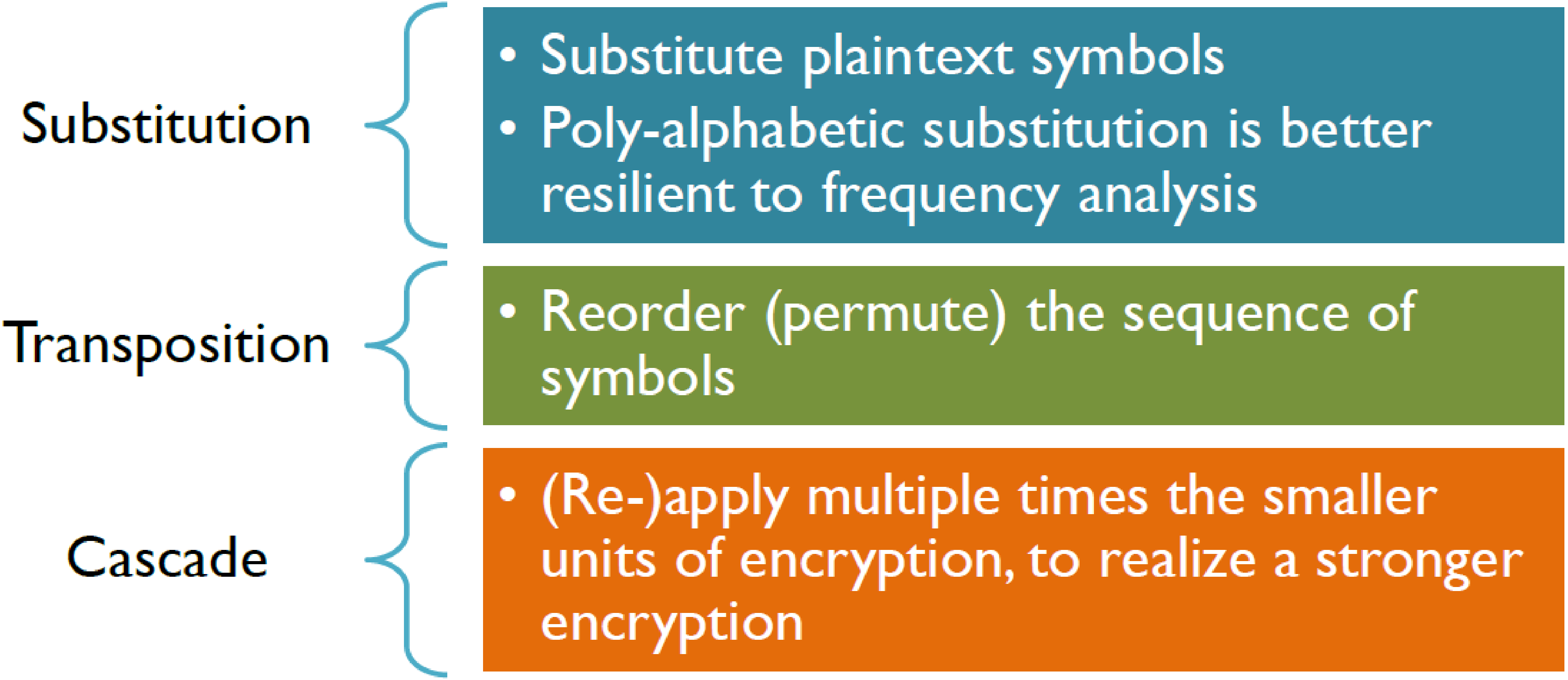
```
Key:          4 3 1 2 5 6 7
Plaintext:    a t t a c k p
              o s t p o n e
              d u n t i l t
              w o a m x y z
```

- Reapply same transposition once more

```
Key:          4 3 1 2 5 6 7
Input:        t t n a a p t
              m t s u o a o
              d w c o i x k
              n l y p e t z
Output:       NSCYAUOPTTWLTMDNAOIEPAXTTOKZ
```

Reapplication makes it harder to

- guess the matrix dimension
- interpolate the column permutation



Substitution

- Substitute plaintext symbols
- Poly-alphabetic substitution is better resilient to frequency analysis

Transposition

- Reorder (permute) the sequence of symbols

Cascade

- (Re-)apply multiple times the smaller units of encryption, to realize a stronger encryption