CEN 448
Security and Internet Protocols
Chapter 2
Classical Encryption Techniques

Dr. Mostafa Hassan Dahshan
Computer Engineering Department
College of Computer and Information Sciences
King Saud University
mdahshan@ccis.ksu.edu.sa

Acknowledgements

- These notes use some slides from WilliamStallings.com website made by Dr. Lawrie Brown
- Imported slides have *Italic Titles*

Symmetric Encryption

- aka conventional, private-key / single-key
- sender and recipient share a common key
- all classical encryption algorithms are private-key
- was only type prior to invention of public-key in 1970's
- and by far most widely used

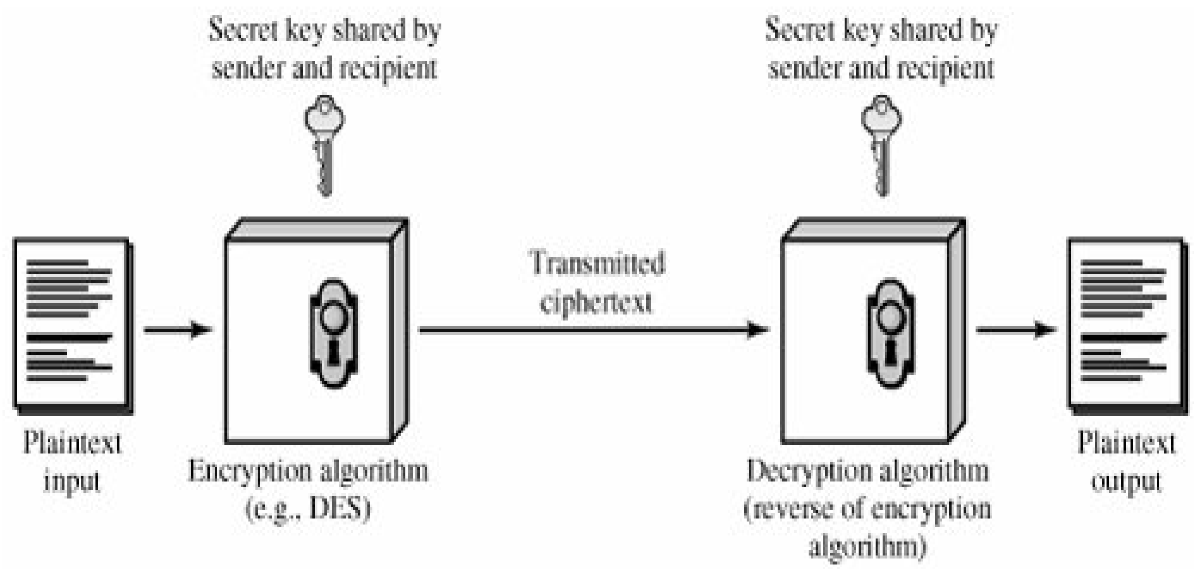
Ingredients

- Plaintext
  - original intelligible message
- Encryption algorithm
  - performs substitutions, transformations
  - input: plaintext, key. output: ciphertext
- Secret Key
  - different keys → different outputs, substitutions and transformations

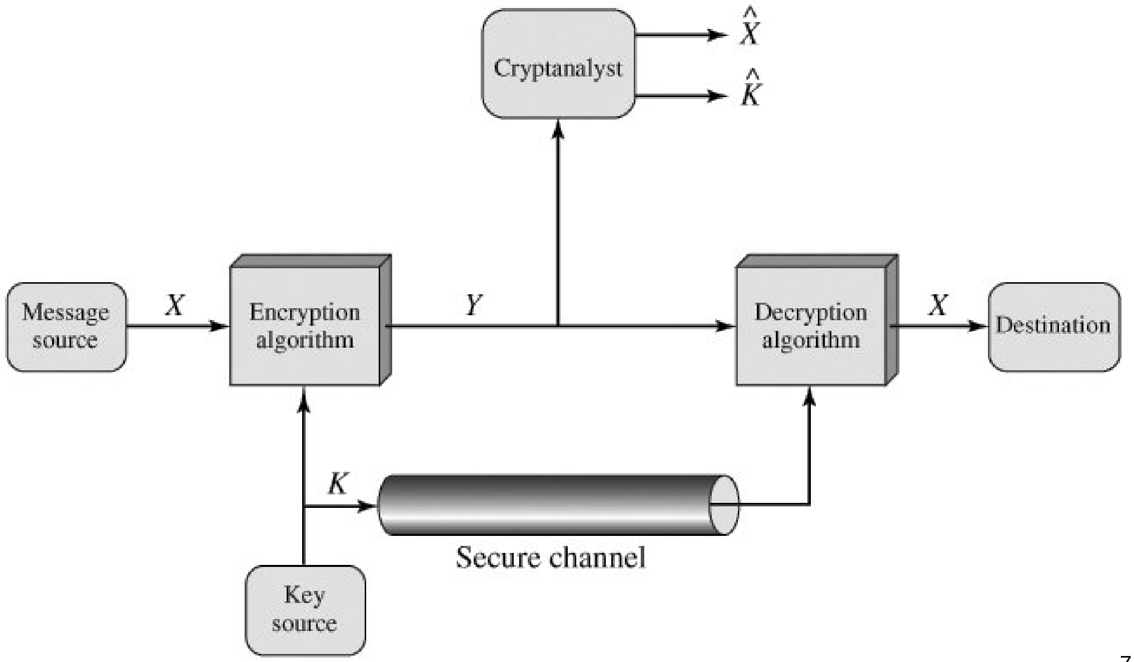
Ingredients

- Cipher text
  - unintelligible scrambled message
  - depend on plaintext and key
- Decryption algorithm
  - encryption algorithm run in reverse
  - input: ciphertext, key. output: plaintext

Simplified Model



Simplified Model



Requirements

- two requirements for secure use of symmetric encryption:
  - a strong encryption algorithm
  - a secret key known only to sender / receiver
- mathematically have:

  $Y = E_K(X)$

  $X = D_K(Y)$
- assume encryption algorithm is known
- implies a secure channel to distribute key

Characterization

- Type of operation
  - substitution: each element of plaintext (bit, character) mapped to another element
  - transposition: plaintext elements rearranged
- Processing method
  - stream cipher: element by element (bit, byte)
  - block cipher: block transformed as a whole

Encryption Attacks

- Cryptanalysis
  - exploit characteristics of algorithm to deduce plaintext or encryption key
  - may use pairs of plaintext, ciphertext
- Brute-force attack
  - try all possible keys on ciphertext
  - on average, half of possible keys tried

Types of Encryption Security

- **unconditional security**
  - cipher cannot be broken
  - no matter how much computer power or time is available
  - ciphertext provides insufficient information to uniquely determine the corresponding plaintext
  - only such cipher: one-time pad
- **computational security**
  - cost of breaking cipher exceeds value of encrypted information
  - time required to break cipher exceeds lifetime of information

Cryptanalysis Attacks

- Attempt to deduce specific plaintext or key
- Rely on
  - nature of algorithm
  - some knowledge of plaintext characteristics
- Examples
  - some file types have common header
  - exploit statistics of human language
  - power consumed by encryption algorithm

Cryptanalysis Attacks

Type of Attack	Known to Cryptanalyst
Ciphertext only	•Encryption algorithm •Ciphertext
Known plaintext	•Encryption algorithm •Ciphertext •One or more plaintext-ciphertext pairs formed with the secret key
Chosen plaintext	•Encryption algorithm •Ciphertext •Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key
Chosen ciphertext	•Encryption algorithm •Ciphertext •Purported ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key
Chosen text	•Encryption algorithm •Ciphertext •Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key •Purported ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key

Brute Force Attacks

- always possible to simply try every key
- most basic attack, proportional to key size
- assume either know / recognise plaintext

Brute Force Attacks

Key size (bits)	Number of alternative keys		Time required at 1 decryption/µs		Time required at 10^6 decryption/µs
32	2^{32}	$= 4.3 \times 10^{9}$	2^{31} µs	= 35.8 minutes	2.15 milliseconds
56	2^{56}	$= 7.2 \times 10^{16}$	2^{55} µs	= 1142 years	10.01 hours
128	2^{128}	$= 3.4 \times 10^{38}$	2^{127} µs	$= 5.4 \times 10^{24}$ years	5.4×10^{18} years
168	2^{168}	$= 3.7 \times 10^{50}$	2^{167} µs	$= 5.9 \times 10^{36}$ years	5.9×10^{30} years
26 characters (permutation)	26!	$= 4 \times 10^{26}$	2×10^{26} µs	$= 6.4 \times 10^{12}$ years	6.4×10^{6} years

Substitution Techniques

- Letters in plaintext is replaced by
  - other letters
  - numbers
  - symbols
- Plaintext bit-sequence is replaced by a ciphertext sequence

Substitution Techniques

- Caesar cipher
- Monoalphabetic ciphers
- Playfair cipher
- Polyalphabetic ciphers
- One-time pad

Caesar Cipher

- Ciphertext letter = plaintext letter + 3
- Letters wrap around, Z is next after A

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

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

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

Caesar Cipher

- $C = E(3, p) = (p + 3) \bmod 26$
- If shift is different from 3
  $C = E(k, p) = (p + k) \bmod 26$
- $p = D(k, C) = (C\ k) \bmod 26$

Brute Force Attack

- Encryption and decryption algorithms are known
- Only 25 keys to try
- Plaintext language is known

KEY	PHHW	PH	DIWHU	WKH	WRJD	SDUWB
1	oggv	og	chvgt	vjg	vqic	rctva
2	nffu	nf	bgufs	uif	uphb	qbsuz
3	meet	me	after	the	toga	party
4	ldds	ld	zesdq	sgd	snfz	ozqsx
5	kccr	kc	ydrcp	rfc	rmey	nyprw
6	jbbq	jb	xcqbo	qeb	qldx	mxoqv
7	iaap	ia	wbpan	pda	pkcw	lwnpu
8	hzzo	hz	vaozm	ocz	ojbv	kvmot
9	gyyn	gy	uznyl	nby	niau	julns
10	fxxm	fx	tymxk	max	mhzt	itkmr
11	ewwl	ew	sxlwj	lzw	lgys	hsjlq
12	dvvk	dv	rwkvi	kyv	kfxr	grikp
13	cuuj	cu	qvjuh	jxu	jewq	fqhjo
14	btti	bt	puitg	iwt	idvp	epgin
15	assh	as	othsf	hvs	hcuo	dofhm
16	zrrg	zr	nsgre	gur	gbtn	cnegl
17	yqqf	yq	mrfqd	ftq	fasm	bmdfk
18	xppe	xp	lqepc	esp	ezrl	alcej
19	wood	wo	kpdob	dro	dyqk	zkbdi
20	vnnc	vn	jocna	cqn	cxpj	yjach
21	ummb	um	inbmz	bpm	bwoi	xizbg
22	tlla	tl	hmaly	aol	avnh	whyaf
23	skkz	sk	glzkx	znk	zumg	vgxze
24	rjjy	rj	fkyjw	ymj	ytlf	ufwyd
25	qiix	qi	ejxiv	xli	xske	tevxc

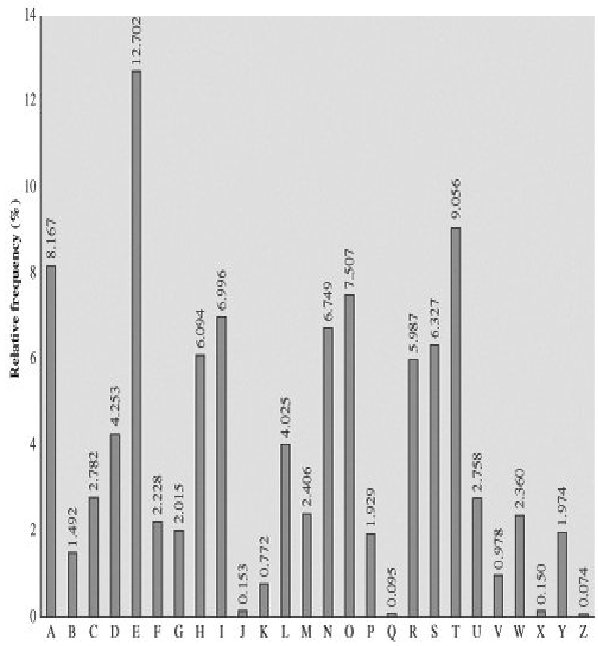
Monoalphabetic Cipher

- Arbitrary substitution of letters
- Number of keys 26×25×…×1 = 26! (Over 4×10^{26})
- Regularities in the language can be exploited

Monoalphabetic – Example

UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ
VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX
EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ

P 13.33	H 5.83	F 3.33	B 1.67	C 0.00
Z 11.67	D 5.00	W 3.33	G 1.67	K 0.00
S 8.33	E 5.00	Q 2.50	Y 1.67	L 0.00
U 8.33	V 4.17	T 2.50	I 0.83	N 0.00
O 7.50	X 4.17	A 1.67	J 0.83	R 0.00
M 6.67				



Monoalphabetic – Example

- Frequency of letters
  - P → e, Z → t
- Frequency of two-letter combinations
  - ZW → th

```
UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ
 t a        e  e te  a that e e a         a
VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX
   e t   ta t ha e ee  a e  th    t  a
EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ
 e  e e tat  e   the   t
```

it was disclosed yesterday that several informal but direct contacts have been made with political representatives of the viet cong in moscow

Playfair Cipher

- 5×5 matrix of letters
- Constructed using a keyword

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

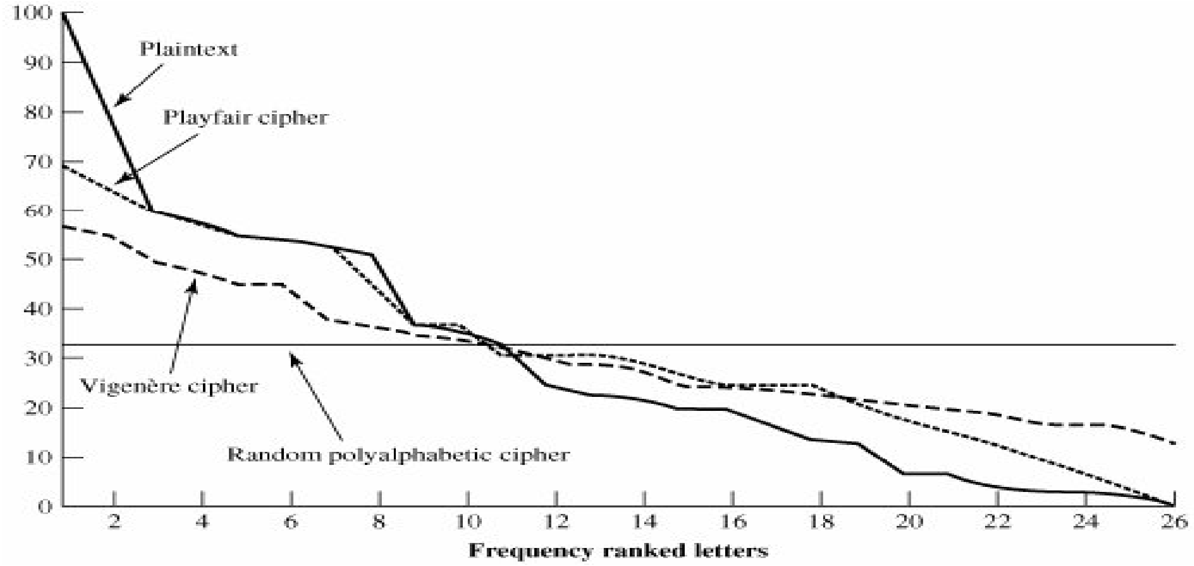
Playfair Cipher

- Plaintext encrypted two letters at a time
- Repeating letters separated by filler "x" e.g. balloon → ba lx lo on
- Letters in same row are each replaced by letter to right. e.g. ar → RM
- Letters in same col are each replaced by letter beneath. e.g. mu → CM
- Otherwise, letter replaced by one in its row and col of the other letter. hs → BP

Playfair Cipher

- Advantages
  - 26×26 diagrams (two letter combinations)
  - Possible keys? (homework ☺)
- Disadvantages
  - still leaves much of language structure
  - few 100s of ciphertext letters are enough for cryptanalysis

Relative Frequency of Letters



Polyalphabetic Ciphers

- **polyalphabetic substitution ciphers**
- improve security using multiple cipher alphabets
- make cryptanalysis harder with more alphabets to guess and flatter frequency distribution
- use a key to select which alphabet is used for each letter of the message
- use each alphabet in turn
- repeat from start after end of key is reached

Vigenère Cipher

- simplest polyalphabetic substitution cipher
- effectively multiple Caesar ciphers
- key is multiple letters long $K = k_1\ k_2\ \ldots\ k_d$
- i^{th} letter specifies i^{th} alphabet to use
- use each alphabet in turn
- repeat from start after d letters in message
- decryption simply works in reverse

Vigenère Cipher

Key	Plaintext																									
	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
a	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
b	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	A
c	C	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
d	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
e	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	D
f	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
g	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
h	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
i	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
j	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
k	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
l	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
m	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
n	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
o	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
p	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
r	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
s	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
t	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
u	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
v	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
w	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
x	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
z	Z	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

Example of Vigenère Cipher

- write the plaintext out
- write the keyword repeated above it
- use each key letter as a Caesar cipher key
- encrypt the corresponding plaintext letter
- eg using keyword *deceptive*

```
key:       deceptivedeceptivedeceptive
plaintext: wearediscoveredsaveyourself
ciphertext:ZICVTWQNGRZGVTWAVZHCQYGLMGJ
```


One-Time Pad

- if a truly random key as long as the message is used, the cipher will be secure
- called a One-Time pad
- is unbreakable since ciphertext bears no statistical relationship to the plaintext
- since for **any plaintext** & **any ciphertext** there exists a key mapping one to other
- can only use the key **once** though
- problems in generation & safe distribution of key

One-Time Pad – Example

- Vigenère scheme with 27 characters
- 27th character is space
- One-time key/message, = message length

```
ciphertext: ANKYODKYUREPFJBYOJDSPLREYIUNOFDOIUERFPLUYTS
key:        pxlmvmsydofuyrvzwc tnlebnecvgdupahfzzlmnyih
plaintext:  mr mustard with the candlestick in the hall

ciphertext: ANKYODKYUREPFJBYOJDSPLREYIUNOFDOIUERFPLUYTS
key:        mfugpmiydgaxgoufhklllmhsqdqogtewbqfgyovuhwt
plaintext:  miss scarlet with the knife in the library
```


Transposition Techniques

- Perform some permutations on plaintext letters
- Examples
  - Rail fence cipher
  - Transposition matrix

Rail Fence Cipher

- Plaintext written as sequence of diagonals
- Read off as sequence of rows

```
m e m a t r h t g p r y
 e t e f e t e o a a t
```

MEMATRHTGPRYETEFETEOAAT

- Trivial to cryptanalyze

Transposition Matrix

- Write message in rectangle, row by row
- Read message off, column by column
- Permute order of columns
- Order of columns is the key

```
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
Ciphertext:    TTNAAPTMTSUOAODWCOIXKNLYPETZ
```

Transposition Matrix

- Original order of letters
  - 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28
- After transposition
  - 03 10 17 24 04 11 18 25 02 09 16 23 01 08 15 22 05 12 19 26 06 13 20 27 07 14 21 28
- Somewhat regular structure

Transposition Matrix

- More than one stage of transposition

```
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
Ciphertext:   TTNAAPTMTSUOAODWCOIXKNLYPETZ
```

```
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
```

- After second transposition
- 17 09 05 27 24 16 12 07 10 02 22 20 03 25 15 13 04 23 19 14 11 01 26 21 18 08 06 28
- Much less structured