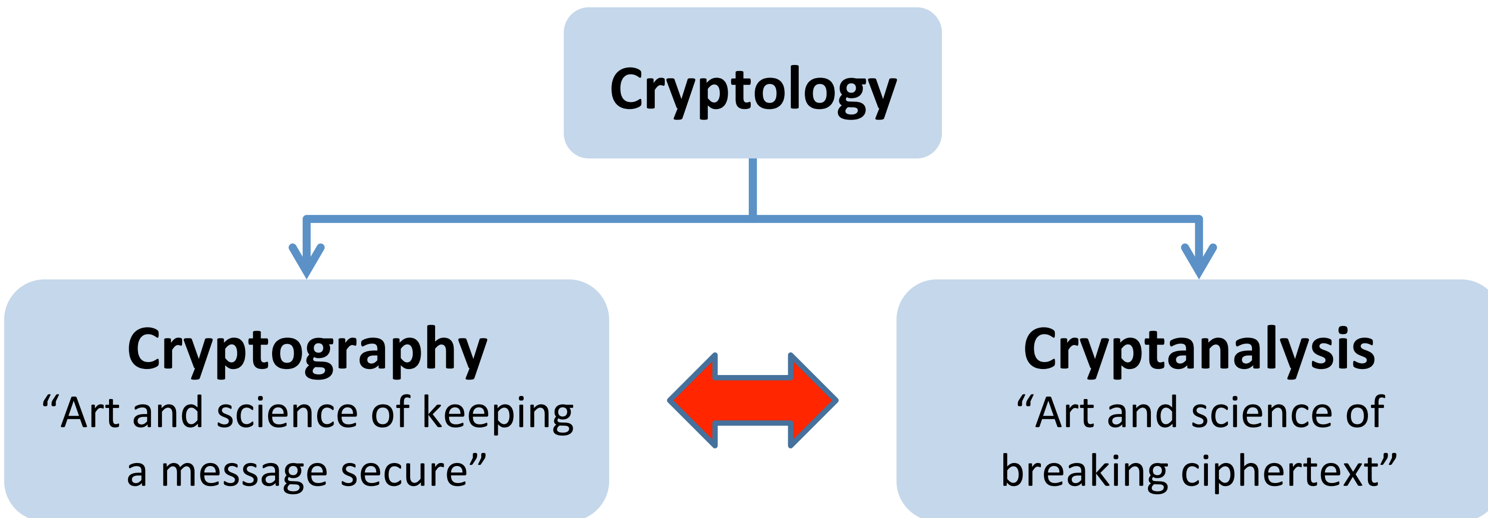
Security
Cryptology

CS3524 Distributed Systems and Security

Lecture 18

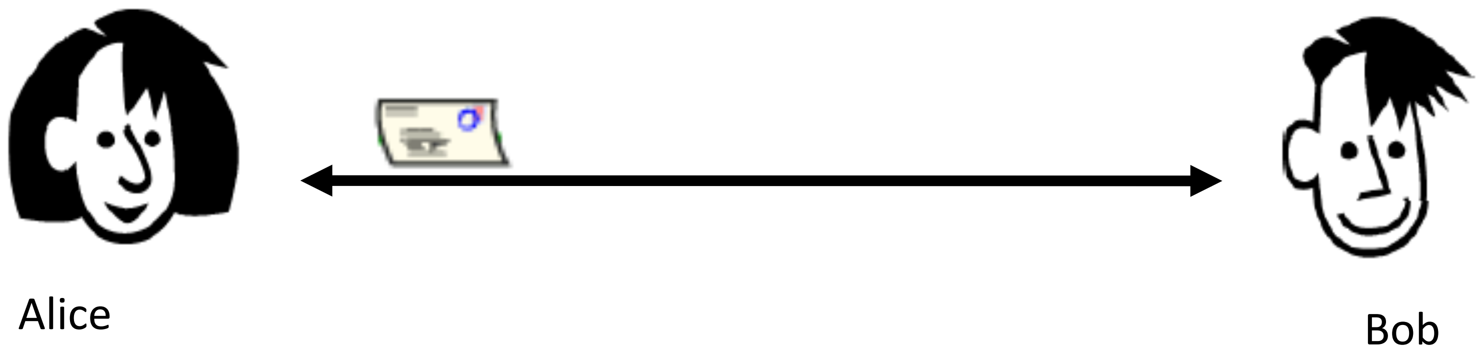
What is Cryptology?



- Cryptology covers two related fields:
  - Cryptography: how to keep a message secure (develop ciphers that are unbreakable)
  - Cryptanalysis: how break ciphers and cipher-text

Cryptography
Why use Cryptography?

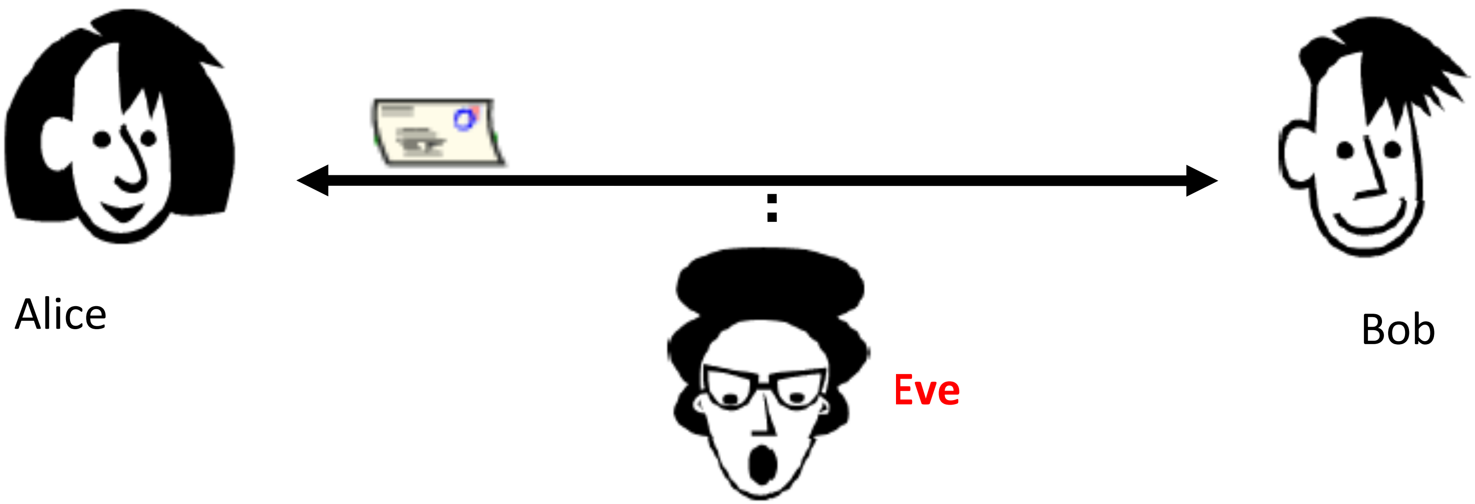
Communication Scenario



Alice and Bob want to communicate

Cryptography
Why use Cryptography?

Threat!!

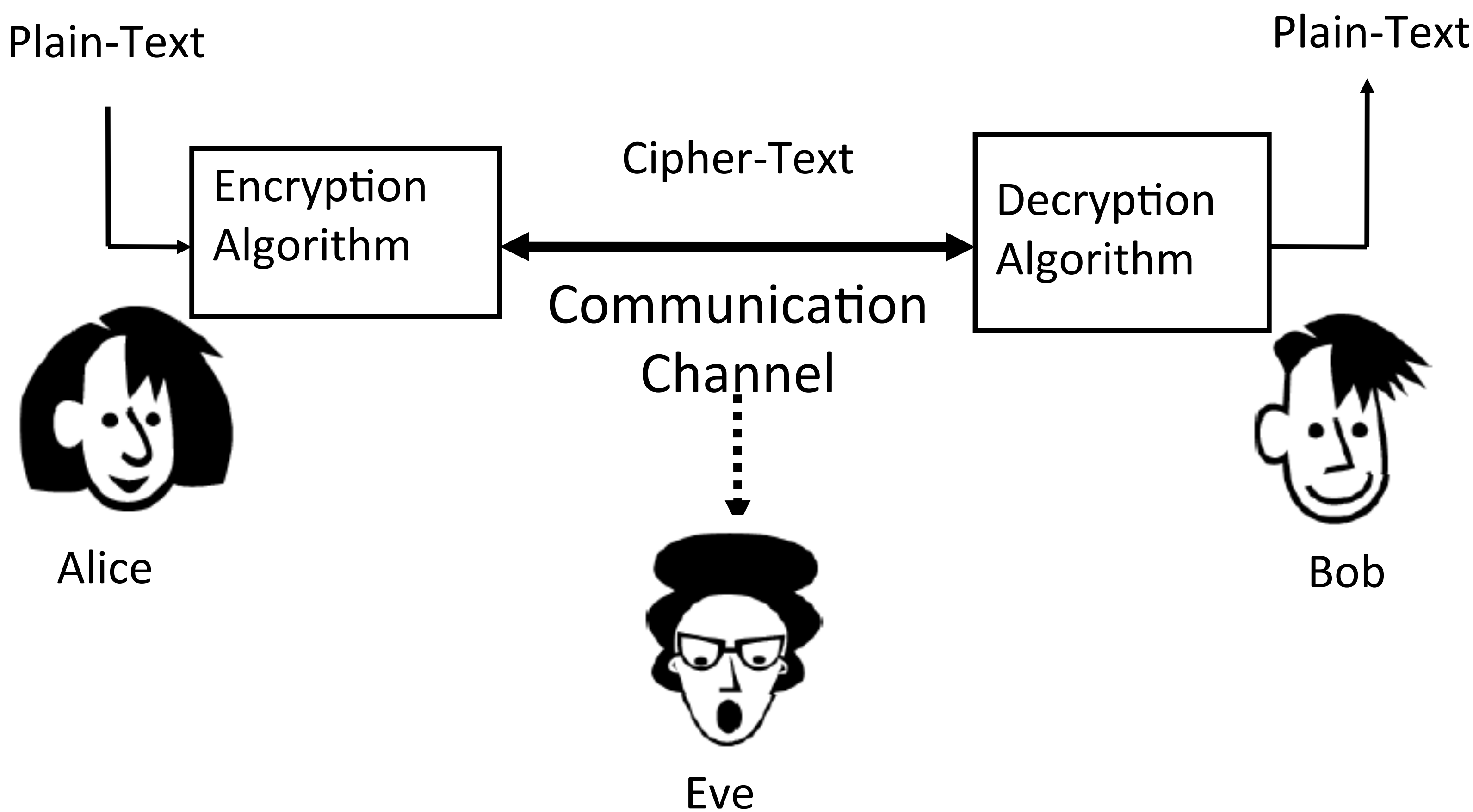


Alice and Bob want to communicate

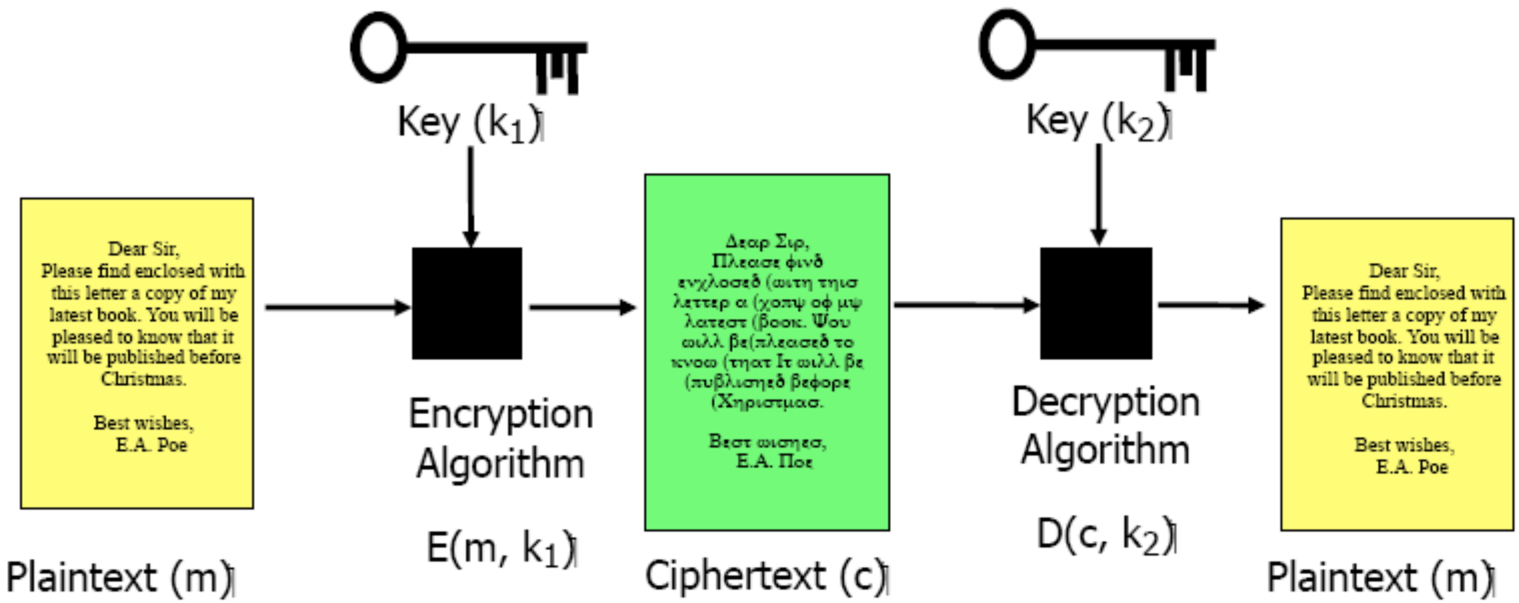
Eve is eavesdropping (intercept, delete, add message)

- Cryptography is needed when communicated messages should be safeguarded against a third party intercepting or manipulating them.

Cryptography Terminology



Cryptography
Encode and Decode with a Cipher



- Cipher = Algorithm + Key
- No cipher should rely on the secrecy of the algorithm!

Basic Principles of Cryptography Cipher Algorithms

- A cipher is an algorithm that scrambles plain text, given a key, into a form that hides its meaning
- Plaintext symbols can be single letters, blocks of letters or complete words
- Two forms of ciphers
  - Substitution ciphers: replace plaintext symbols with corresponding cipher-text symbols
  - Transposition ciphers: reorder plaintext symbols within the cipher-text

Transposition Cipher

- A transposition cipher is a method of encryption where symbols of the plaintext are reordered according to a particular scheme
- There are different forms of Transposition Cipher
  - Rail Fence cipher, Route cipher, Columnar Transposition
- Columnar Transposition:
  - The plaintext is written out in rows of fixed length, generating a matrix
  - Cipher: an encoded form of the text is generated by reading out and concatenating the columns of this matrix, where the columns may be chosen in some scrambled order
  - The length of the rows and the scrambling (permutation) of the columns is usually defined by a keyword
    - E.g.: the word "ZEBRAS" is of length 6 (length of rows) and the letters have the following alphabetical order "6 3 2 4 1 5" (determining how the columns have to be read in sequence
- Problem with Transposition Cipher:
  - Cannot produce output until all input characters have been read

Transposition Cipher
Columnar Transposition

- Plaintext:

MESSAGE FROM MARY STUART KILL THE QUEEN

Plaintext in

1	2	3	4	5	6	7	8	9
M	E	S	S	A	G	E	F	R
O	M	M	A	R	Y	S	T	U
A	R	T	K	I	L	L	T	H
E	Q	U	E	E	N			

Ciphertext out

- Ciphertext: **MOAEEMRQSMTUSAKEARIEGYLNESLFTTRUH**

MOAEE MRQSM TUSAK EARIE GYLNE SLFTT RUH

Transposition Cipher
Columnar Transposition

- Plaintext:

MESSAGE FROM MARY STUART KILL THE QUEEN

Plaintext in

4	9	1	7	5	3	2	8	6
M	E	S	S	A	G	E	F	R
O	M	M	A	R	Y	S	T	U
A	R	T	K	I	L	L	T	H
E	Q	U	E	E	N			

With 9 columns, we have 9! = 362,880 possible keys

Ciphertext out

- Ciphertext: **SMTUESLGYLNMOAEARIERUHSAKEFTTEMRQ**

SMTUE SLGYL NMOAE ARIER UHSAK EFTTE MRQ

Transposition Cipher

- How to decode:
  - We know: key has length 9
  - We know: cipher text has length 33
  - How many rows do we need in transposition table?
- Therefore
  - Ciphertext-length / Keylength = 33 / 9 = 3.6
    - We round this number up to 4, therefore we need a table with 4 rows
  - However: last row is not full, how many empty spaces?
    - We calculate: Rows x Keylength – Ciphertextlength = 4 x 9 – 33 = 3
    - Therefore: the last row has 3 empty spaces (and 6 full)

Transposition Cipher
Columnar Transposition

- Plaintext: using the word “SECRET” as a key
  - defines number of columns for the transposition table
    - The key has 6 letters, therefore 6 columns
  - Defines the column sequence during readout
    - According to the alphabet, the letter C corresponds to “1”, E to “2” and “3” (as it occurs two times), R to “4”, S to “5” and T to “6”
    - The key “SECRET”, therefore, defines a read-out sequence of “5 2 1 4 3 6” for the table columns to generate the cipher text

S	E	C	R	E	T
5	2	1	4	3	6
M	E	S	S	A	G
E	F	R	O	M	M
A	R	Y	S	T	U
A	R	T	K	I	L
L	T	H	E	Q	U
E	E	N			

With 6 columns, we have 6! = 720 possible keys

Transposition Cipher
Columnar Transposition

- Plaintext: using “SECRET” as a key

MESSAGE FROM MARY STUART KILL THE QUEEN

“SECRET” = 521436

Plaintext in

S	E	C	R	E	T
5	2	1	4	3	6
M	E	S	S	A	G
E	F	R	O	M	M
A	R	Y	S	T	U
A	R	T	K	I	L
L	T	H	E	Q	U
E	E	N			

Ciphertext out

SRYTHNEFRRTEAMTIQSOSKEMEAALEGMULU

SRYTH NEFRR TEAMT IQSOS KEMEA ALEGM ULU

Transposition Cipher

- How to decode:
  - We know: key is “SECRET”, has length 6
  - We know: cipher text is of length 33
  - How many rows do we need in transposition table?
- Therefore
  - Ciphertext-length / Keylength = 33 / 6 = 5.5
    - We always round up: with 5.5 as a result, we need a table with 6 rows
  - However: last row is not full, how many empty spaces?
    - We calculate: Rows x Keylength – Ciphertextlength = 6 x 6 – 33 = 3
    - Therefore: the last row has 3 empty spaces (and 3 full)

Transposition Cipher
Columnar Transposition

- Decryption: using “SECRET” as a key
  - We know: first three columns have 6 rows
  - Fill ciphertext into columns according to column numbers

SRYTH NEFRR TEAMT IQSOS KEMEA ALEGM ULU

Ciphertext in

First, column 3:

S	E	C	R	E	T
5	2	1	4	3	6
		S			
		R			
		Y			
		T			
		H			
		N			

Transposition Cipher
Columnar Transposition

- Decryption: using “SECRET” as a key
  - We know: first three columns have 6 rows
  - Fill ciphertext into columns according to column numbers

SRYTH NEFRR TEAMT IQSOS KEMEA ALEGM ULU

Ciphertext in

Second, column 2:
Etc.

S	E	C	R	E	T
5	2	1	4	3	6
	E	S			
	F	R			
	R	Y			
	R	T			
	T	H			
	E	N			

Transposition Cipher
Columnar Transposition

- Decryption: using “SECRET” as a key

SRYTH NEFRR TEAMT IQSOS KEMEA ALEGM ULU

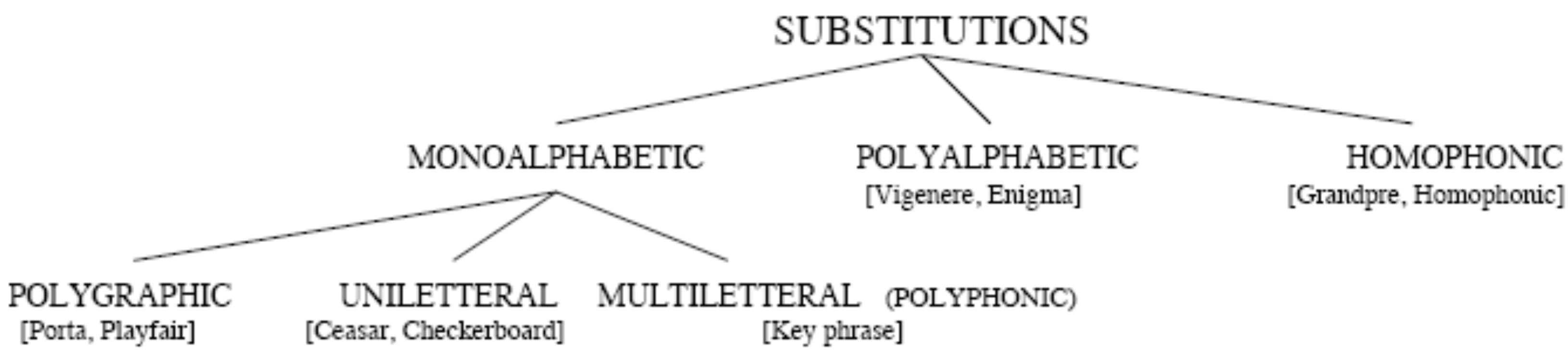
Ciphertext in

S	E	C	R	E	T
5	2	1	4	3	6
M	E	S	S	A	G
E	F	R	O	M	M
A	R	Y	S	T	U
A	R	T	K	I	L
L	T	H	E	Q	U
E	E	N			

Plantext out

MESSAGE FROM MARY STUART KILL THE QUEEN

Substitution Ciphers



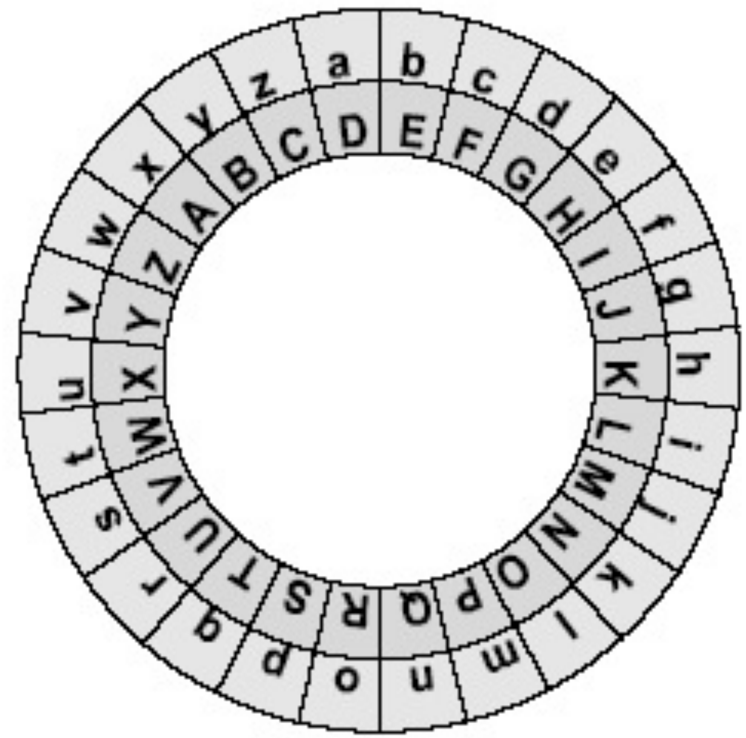
- The basic idea for Substitution Ciphers is to substitute one symbol in the plain text with another symbol in the ciphertext

Substitution Cipher

- Mono-alphabetic Substitution
  - One symbol in plaintext is substituted by one symbol (always the same) in ciphertext
  - Easy to attack: Frequency of occurrence of a particular letter is mirrored in ciphertext, with the use of frequency analysis (frequency tables) easy to decipher

Cesar Cipher
Mono-Alphabetic Substitution Cipher

- Cipher attributed to Julius Caesar
- Cipher algorithm:
  - Shift each letter in the plaintext n places
  - Each plaintext letter is replaced with the same symbol throughout the text
- With an alphabet of 26 characters, we have 25 different shift ciphers



- Example
  - Try to encode: “treaty impossible”
  - Try to decode: DWWDFN DW GDZQ

Mono-Alphabetic Substitution Cipher

Caesar's Cipher, "Key" is number of Shifts

- Plaintext:

MESSAGE FROM MARY STUART KILL THE QUEEN

- Substitution table: Caesar's Cipher
  - Given: "key = 3": construct the substitution table by shifting the alphabet three characters to the left:

ABCDEFGHIJKLMNOPQRSTUVWXYZ

DEFGHIJKLMNOPQRSTUVWXYZABC

key = 3

- Ciphertext:

PHVVDJH IURP PDUB VWXDUW NLOO WKH TXHHQ

Mono-Alphabetic Substitution Cipher

Key Phrase Substitution Table

- Plaintext:

MESSAGE FROM MARY STUART KILL THE QUEEN

- Substitution table: Use a key phrase
  - Given: “key = SCOTLAND”: construct the substitution table with the key and add the rest of the alphabet – each character can only occur once, even in the key!

ABCDEFGHIJKLMNOPQRSTUVWXYZ

SCOTLANDBEFGHIJKMPQRUVWXYZ key = SCOTLAND

- Ciphertext:

HLQQSNL APJH HSPY QRUSPR FBGG RDL MULLI

Mono-Alphabetic Substitution Cipher

Random Substitution Table

- Plaintext:

MESSAGE FROM MARY STUART KILL THE QUEEN

- Substitution table: Use a random sequence of the characters of the alphabet:
  - The key is the sequence of the 26 characters, in random order

ABCDEFGHIJKLMNOPQRSTUVWXYZ

EYUOBMDXVTHIJPRCNAKQLSGZFW

26! possible keys

- Ciphertext:

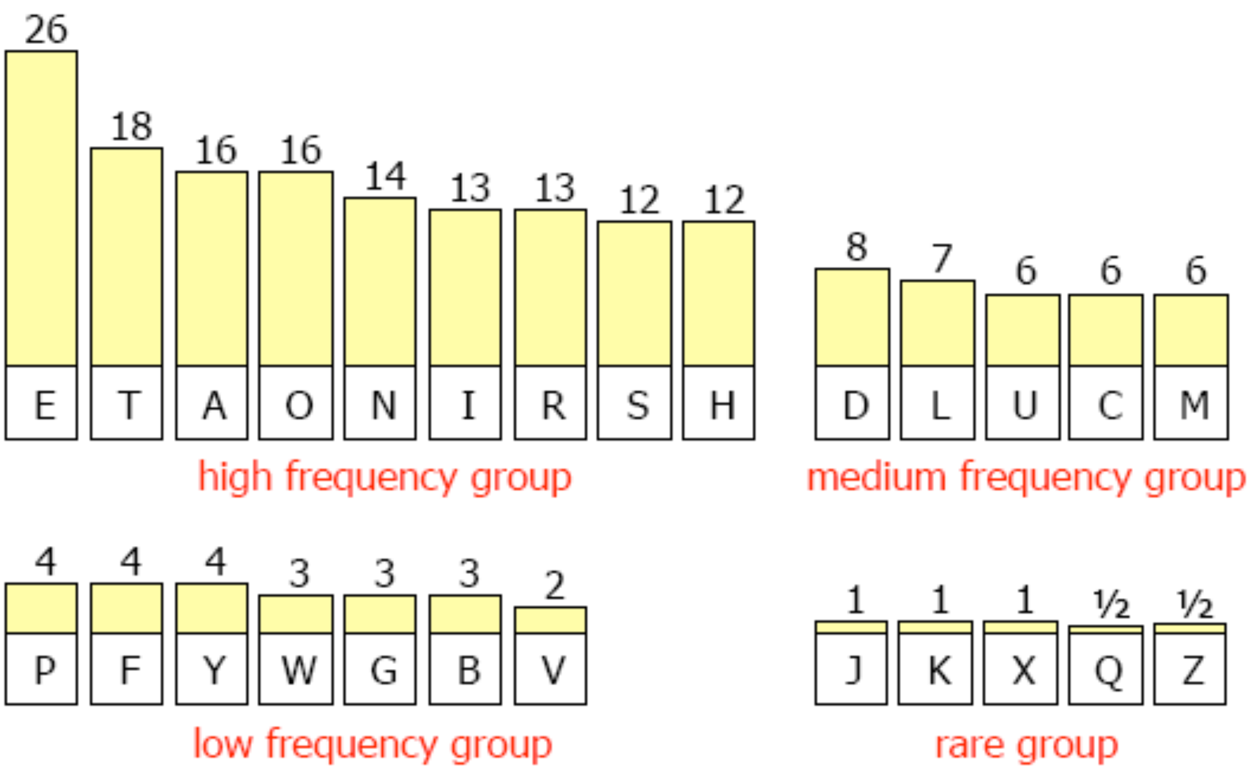
JBKKEDB MARJ JEAF KQLEAQ HVII QXB NLBBP

Frequency Analysis
Cryptanalysis of Substitution Ciphertext

- Attempt to decipher substitution ciphertext
- In English:
  - Most common letters: E, T, A, O, N, I, ...
  - Most common 2-letter words: ON, AS, TO, AT, IT, ...
  - Most common 3-letter words: THE, AND, FOR, WAS, ...
- Letter frequencies in ciphertext can be used to guess plaintext letters
  - Statistical Frequency Analysis of letters and words can easily break any mono-alphabetic substitution cipher

Frequency Analysis

- Example: an analysis of 200 English letters results in the following Frequency Table:



Georges Perec, "La disparition", 1969

Book of 280 pages without a single letter e

…Anton Voyl n'arrivait pas à dormir. Il alluma. Son Jaz marquait minuit vingt. Il poussa un profond soupir, s'assit dans son lit, s'appuyant sur son polochon. Il prit un roman, il l'ouvrit, il lut ; mais il n'y saisit qu'un imbroglio confus, il butait à tout instant sur un mot dont il ignorait la signification. Il abandonna son roman sur son lit. Il alla à son lavabo ; il mouilla un gant qu'il passa sur son front, sur son cou. Son pouls battait trop fort. Il avait chaud…

Use Frequency Analysis

Try to decode the following Ciphertext:

```
ORITFSIMU YKFMUNM WIUNIS UEI HFKK RIMIXFMD UEI PVUENRFUA NC
--------- ------- ------ --- ---- -------- --- --------- --
UEI MPUFNM'T FMUIKKFDIMYI PDIMYFIT HIYPVTI FU YNMUPFMT XEPU
--- ------'- ------------ -------- ------- -- -------- ----

EI YPKKIS P ORNWFTFNM UEPU XNVKS LPJI FU P YRFLI CNR P
-- ------ - --------- ---- ----- ---- -- - ----- --- -
DNWIRMLIMU NCCFYFPK UN SFTYKNTI YKPTTFCFIS FMCNRLPUFNM.
---------- -------- -- -------- ---------- -----------.
```

Based on the Frequency Table given, we assume that the letter with the highest frequency in the Ciphertext encodes the letter 'e'

Use Frequency Analysis

Try to decode the following Ciphertext:

```
ORITFSIMU YKFMUNM WIUNIS UEI HFKK RIMIXFMD UEI PVUENRFUA NC
--e---e-- ------- -e--e- --e ---- -e-e---- --e --------- --
UEI MPUFNM'T FMUIKKFDIMYI PDIMYFIT HIYPVTI FU YNMUPFMT XEPU
--e ------'- ---e----e--e --e---e- -e----e -- -------- ----

EI YPKKIS P ORNWFTFNM UEPU XNVKS LPJI FU P YRFLI CNR P
-e ----e- - --------- ---- ----- ---e -- - ----e --- -
DNWIRMLIMU NCCFYFPK UN SFTYKNTI YKPTTFCFIS FMCNRLPUFNM.
---e---e-- -------- -- -------e --------e- -----------.
```

Based on the Frequency Table given, we assume that the letter with the highest frequency in the Ciphertext encodes the letter 'e'

Use Frequency Analysis

Step 1:

```
ORITFSIMU YKFMUNM WIUNIS UEI HFKK RIMIXFMD UEI PVUENRFUA NC
-e---e-t ----t-- -et-e- the ---- -e-e---- the --th---t- --
UEI MPUFNM'T FMUIKKFDIMYI PDIMYFIT HIYPVTI FU YNMUPFMT XEPU
the --t---'- --te----e--e --e---e- -e----e -t -------- -h-t

EI YPKKIS P ORNWFTFNM UEPU XNVKS LPJI FU P YRFLI CNR P
he ----e- - --------- th-t ----- ---e -t - ----e --- -
DNWIRMLIMU NCCFYFPK UN SFTYKNTI YKPTTFCFIS FMCNRLPUFNM.
---e---e-t -------- t- -------e --------e- -------t---.
```

We can identify:

U	**=**	**t**
E	**=**	**h**
I	**=**	**e**

Use Frequency Analysis

Step 2:

```
ORITFSIMU YKFMUNM WIUNIS UEI HFKK RIMIXFMD UEI PVUENRFUA NC
--e---e-t ----t-- -et-e- the ---- -e-e---- the a-th---t- --
UEI MPUFNM'T FMUIKKFDIMYI PDIMYFIT HIYPVTI FU YNMUPFMT XEPU
the -at---'- --te----e--e a-e---e- -e-a--e -t ---ta--- -hat

EI YPKKIS P ORNWFTFNM UEPU XNVKS LPJI FU P YRFLI CNR P
he -a--e- a --------- that ----- -a-e -t a ----e --- a
DNWIRMLIMU NCCFYFPK UN SFTYKNTI YKPTTFCFIS FMCNRLPUFNM.
---e---e-t ------a- t- -------e --a-----e- ------at---.
```

P = a

Step 3:

```
ORITFSIMU YKFMUNM WIUNIS UEI HFKK RIMIXFMD UEI PVUENRFUA NC
--e-i-e-t --i-to- -etoe- the -i-- -e-e-i-- the a-tho-it- o-
UEI MPUFNM'T FMUIKKFDIMYI PDIMYFIT HIYPVTI FU YNMUPFMT XEPU
the -atio-'- i-te--i-e--e a-e--ie- -e-a--e it -o-tai-- -hat

EI YPKKIS P ORNWFTFNM UEPU XNVKS LPJI FU P YRFLI CNR P
he -a--e- a --o-i-io- that -o--- -a-e it a --i-e -o- a
DNWIRMLIMU NCCFYFPK UN SFTYKNTI YKPTTFCFIS FMCNRLPUFNM.
-o-e---e-t o--i-ia- to -i---o-e --a--i-ie- i--o--atio-.
```

F = i
N = o

Use Frequency Analysis

Step 4:

```
ORITFSIMU YKFMUNM WIUNIS UEI HFKK RIMIXFMD UEI PVUENRFUA NC
-re-i-e-t --i-to- -etoe- the -i-- re-e-i-- the a-thorit- of
UEI MPUFNM'T FMUIKKFDIMYI PDIMYFIT HIYPVTI FU YNMUPFMT XEPU
the -atio-'- i-te--i-e--e a-e--ie- -e-a--e it -o-tai-- -hat
```

```
EI YPKKIS P ORNWFTFNM UEPU XNVKS LPJI FU P YRFLI CNR P
he -a--e- a -ro-i-io- that -o--- -a-e it a -ri-e for a
DNWIRMLIMU NCCFYFPK UN SFTYKNTI YKPTTFCFIS FMCNRLPUFNM.
-o-er--e-t offi-ia- to -i---o-e --a--ifie- i-for-atio-.
```

C = f
R = r

Step 5:

```
ORITFSIMU YKFMUNM WIUNIS UEI HFKK RIMIXFMD UEI PVUENRFUA NC
-re-i-e-t cli-to- -etoe- the -ill re-e-i-- the authority of
UEI MPUFNM'T FMUIKKFDIMYI PDIMYFIT HIYPVTI FU YNMUPFMT XEPU
the -atio-'- i-telli-e-ce a-e-cie- -ecau-e it co-tai-- -hat
```

```
EI YPKKIS P ORNWFTFNM UEPU XNVKS LPJI FU P YRFLI CNR P
he calle- a -ro-i-io- that -oul- -a-e it a cri-e for a
DNWIRMLIMU NCCFYFPK UN SFTYKNTI YKPTTFCFIS FMCNRLPUFNM.
-o-er--e-t official to -i-clo-e cla--ifie- i-for-atio-.
```

Y = c
K = l
V = u
A = y

Use Frequency Analysis

Step 6:

O	=	p
T	=	s
S	=	d
M	=	n
L	=	m

```
ORITFSIMU YKFMUNM WIUNIS UEI HFKK RIMIXFMD UEI PVUENRFUA NC
president clinton -etoed the -ill rene-in- the authority of
UEI MPUFNM'T FMUIKKFDIMYI PDIMYFIT HIYPVTI FU YNMUPFMT XEPU
the nation's intelli-ence a-encies -ecause it contains -hat

EI YPKKIS P ORNWFTFNM UEPU XNVKS LPJI FU P YRFLI CNR P
he called a pro-ision that -ould ma-e it a crime for a
DNWIRMLIMU NCCFYFPK UN SFTYKNTI YKPTTFCFIS FMCNRLPUFNM.
-o-ernment official to disclose classified information.
```

Step 7:

W	=	v
H	=	b
D	=	g
M	=	n
L	=	m
X	=	w
J	=	k

```
ORITFSIMU YKFMUNM WIUNIS UEI HFKK RIMIXFMD UEI PVUENRFUA NC
president clinton vetoed the bill renewing the authority of
UEI MPUFNM'T FMUIKKFDIMYI PDIMYFIT HIYPVTI FU YNMUPFMT XEPU
the nation's intelligence agencies because it contains what

EI YPKKIS P ORNWFTFNM UEPU XNVKS LPJI FU P YRFLI CNR P
he called a provision that would make it a crime for a
DNWIRMLIMU NCCFYFPK UN SFTYKNTI YKPTTFCFIS FMCNRLPUFNM.
government official to disclose classified information.
```

Mono-alphabetic Substitution Ciphers Polygram

- Polygrams are groups of characters that are substituted by other groups of characters
  - Digrams: groups of 2 characters are substituted by corresponding cipher Digrams
  - Trigrams: groups of 3 characters are substituted by corresponding cipher Trigrams
  - Generally: *n*-grams are substituted by corresponding cipher n-grams
- The key space is extremely large: in full Digram substitution over an alphabet of 26 characters, there are 26! possible keys
- The first practical historical use in 1854 by Sir Charles Wheatstone:
  - Called the “Playfair” cipher

Homophonic Substitution Cipher

- Motivation
  - Increase the difficulty of frequency analysis attacks on substitution ciphers
- Method
  - Plaintext letters map to more than one ciphertext symbol to make it more ambiguous (a one-to-many mapping)
  - Highest-frequency plaintext symbols are given more equivalents than others
  - More than 26 characters will be required in the ciphertext alphabet – expansion becomes necessary
- History
  - Used between 15^{th} and 18^{th} century for diplomatic mail
  - Louis XIV “Great Cipher” was unbreakable for 200 years

Improving Mono-alphabetic Substitution

- How to increase the security of this cipher:
  - Eliminate spaces
  - Use many-to-one mappings that level the frequencies (homophonic)
  - Lots of other clever ideas ...
- Even with these improvements, mono-alphabetic substitutions are still very weak! Can easily be beaten
- Next big step: poly-alphabetic substitution ciphers
  - These were ok until the dawn of modern computers

Poly-Alphabetic Substitution Ciphers

- Uses multiple mono-alphabetic ciphers
  - We use *n* different mono-alphabetic ciphers
  - For each symbol in plaintext, decide which cipher to use
    - May depend on the position of the symbol in plaintext
- Are mostly *periodic* substitution ciphers
  - if we have *n* ciphers, we will apply them in sequence to the first n symbols in plaintext, after that we repeat this sequence of ciphers for the next n symbols etc.

Vigenère Poly-alphabetic Substitution Cipher

plaintext alphabet

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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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

Vigenère square (1586)

Vigenère Poly-alphabetic Substitution Cipher

plaintext alphabet

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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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

Vigenère square (1586)

Keyword: **WHITE**

Vigenère Poly-alphabetic Substitution Cipher

	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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

plaintext alphabet

Vigenère square (1586)

Keyword: **WHITE**

MESSAGE FROM ....

WHITEWH ITEW HITE

Vigenère Poly-alphabetic Substitution Cipher

	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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

plaintext alphabet

Vigenère square (1586)

Keyword: **WHITE**

MESSAGE FROM ....

WHITEWH ITEW HITE

I

Vigenère Poly-alphabetic Substitution Cipher

	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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

plaintext alphabet

Vigenère square (1586)

Keyword: **WHITE**

MESSAGE FROM ....

WHITEWH ITEW HITE

IL

Vigenère Poly-alphabetic Substitution Cipher

	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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

plaintext alphabet

Vigenère square (1586)

Keyword: **WHITE**

MESSAGE FROM ....

WHITEWH ITEW HITE

ILALECL NKSI

How to break the Vigenère Cipher

- Was regarded as practically unbreakable for 300 years
- But: depending on the length n of the keyword, every nth letter in the ciphertext is encrypted by the same alphabet
- Attack
  - Work out the length of the keyword
  - Use frequency analysis to solve the resulting simple substitutions

Working out the Length of the Keyword

```
Plaintext:     tobeornottobe
Keyword:       KEYKEYKEYKEYK
Ciphertext:    DSZOSPXSRDSZO
```

Position 1 Position 10

Distance: 10 – 1 = 9
Factors of 9: 3 and 9, therefore, key has either length 3 or 9

- Repetition of digraphs: DS, SZ, ZO
- We can assume that repeated digraphs in ciphertext correspond to repetitions in plaintext – they are encoded by same section of the key
- Conclusion: length of key is a factor of the distance between occurrences of these digraphs

Longer Key?

- Make key longer: as long as the message itself?

Keyword	VOTINGISIMPORTANTFOR...
Plaintext	ihavethreestinkydogs...
Ciphertext	DVTDRZPJMQPHAGKLWTUJ...

- If there are patterns in the key (e.g., words), the message can still be decrypted with a bit of work

One Time Pad

IF

the key is as long as the message

AND

the key is completely random

THEN

the encryption is perfect (can’t be broken)

- Such a key can only be used once
- Is called a “One Time Pad”

The Use of Modern Computers

- Computers are tailor-made for both code making and breaking - computing engines were spawned from code breaking efforts during WWII (Alan Turing)
- Possible encoding techniques
  - Represent messages as list of numbers (bits) and operate on these with favourite algorithm
- Simplest Case: use Exclusive OR (Vernam, AT&T, 1917)

$$0 \oplus 0 = 0$$
$$1 \oplus 0 = 1$$
$$0 \oplus 1 = 1$$
$$1 \oplus 1 = 0$$

```
A = 1010
B = 1011
C = 1100
D = 1101
E = 1110
F = 1111
```

```
Plaintext   DEAD        1101 1110 1010 1101
Key         BEEF        1011 1110 1110 1111
                        ⊕
Ciphertext              0110 0000 0100 0010 = 6042
```

Symmetric Key Encryption

```
 Plaintext   DEAD         1101 1110 1010 1101
       Key   BEEF      ⊕  1011 1110 1110 1111
Ciphertext             =  0110 0000 0100 0010 = 6042

Ciphertext   6042         0110 0000 0100 0010
       Key   BEEF      ⊕  1011 1110 1110 1111
 Plaintext             =  1101 1110 1010 1101 = DEAD
```

- Is simple: same key to encode and decode

Secure Key?

- Just generate a long "one time pad" bitstream, do the simple XOR, and we have perfect security
- This has two problems
  - It is hard to generate a long truly random bitstream
  - Sender and receiver must both have the same one time pad (i.e. the key)
- If we make the algorithm more sophisticated we can make the minimum length of a secure key much shorter

Strength of Cryptographic Algorithms

- Cryptographic algorithms are classified according to whether they can resist attacks
- Adversarial Models
  - Ciphertext-only attacks (weakest)
    - Attacker has access to encrypted data (e.g. wiretapping), but nothing else
  - Known plaintext attacks (stronger)
    - Attacker obtains the ciphertext and may succeed in getting or guessing all or part of the encrypted plaintext
  - Chosen plaintext attacks (strongest)
    - Attacker can play with encryption device, can choose plaintext to encrypt and may examine the resulting ciphertext