Classical Ciphers

Dhananjoy Dey

Indian Institute of Information Technology, Lucknow
ddey@iiitl.ac.in

January 19, 2021

Disclaimers

All the pictures used in this presentation are taken from freely available websites.

Disclaimers

All the pictures used in this presentation are taken from freely available websites.

If there is a reference on a slide all of the information on that slide is attributable to that source whether quotation marks are used or not.

Disclaimers

All the pictures used in this presentation are taken from freely available websites.

If there is a reference on a slide all of the information on that slide is attributable to that source whether quotation marks are used or not.

Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement nor does it imply that the products mentioned are necessarily the best available for the purpose.

Outline

Outline

Keyword Columnar Transposition

- The columnar transposition cipher can be strengthened by using a keyword
- **Plaintext:** CRYPTOISFUN, **Keyword:** MATH

Keyword Columnar Transposition

- The columnar transposition cipher can be strengthened by using a keyword
- **Plaintext:** CRYPTOISFUN, **Keyword:** MATH

M	A	T	H
C	R	Y	P
T	O	I	S
F	U	N	X

- **Ciphertext:**

Keyword Columnar Transposition

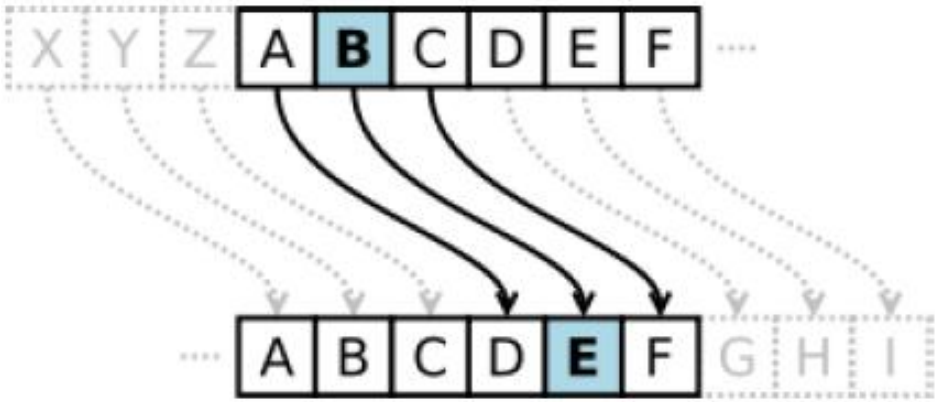
- The columnar transposition cipher can be strengthened by using a keyword
- **Plaintext:** CRYPTOISFUN, **Keyword:** MATH

M	A	T	H
C	R	Y	P
T	O	I	S
F	U	N	X

- **Ciphertext:** ROUPSXCTFYIN

Caesar's Cipher(50 B.C.)

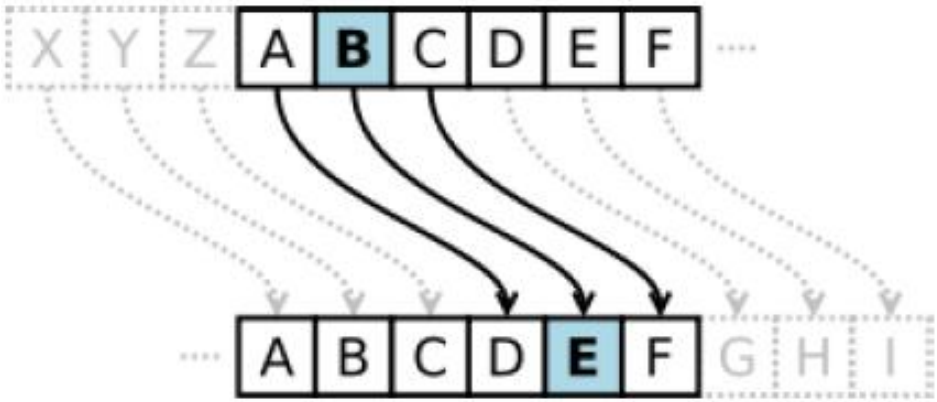
- Used by Caesar to communicate with his generals.
- Each letter is shifted by a constant ($= 3$) position in the alphabet.



E.g., LUCKNOW $\rightarrow$

Caesar's Cipher(50 B.C.)

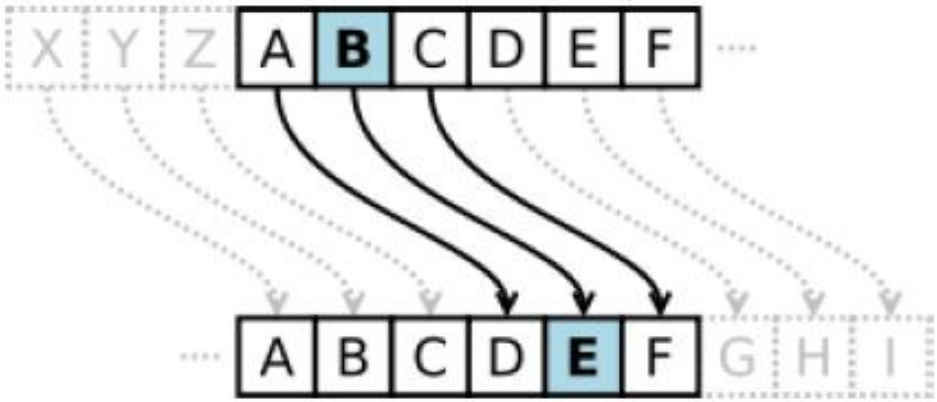
- Used by Caesar to communicate with his generals.
- Each letter is shifted by a constant ($= 3$) position in the alphabet.



E.g., LUCKNOW $\rightarrow$ OXFNQRZ

Caesar's Cipher(50 B.C.)

- Used by Caesar to communicate with his generals.
- Each letter is shifted by a constant ($= 3$) position in the alphabet.

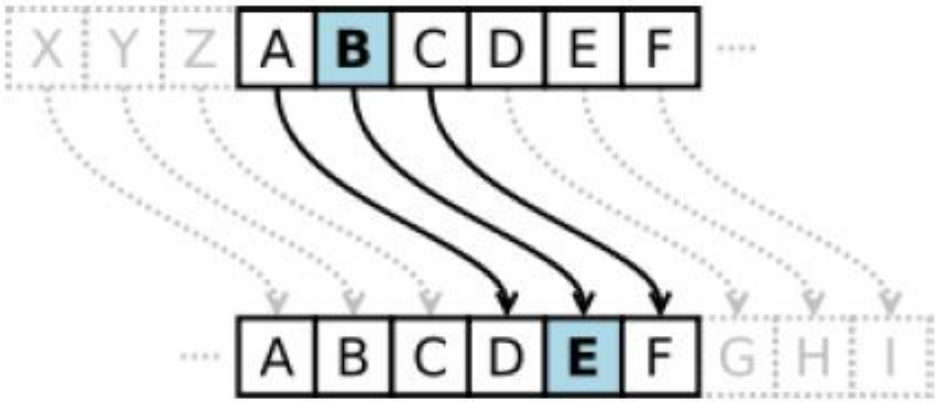


E.g., LUCKNOW $\rightarrow$ OXFNQRZ

- Shift cipher
- # of possibilities

Caesar's Cipher(50 B.C.)

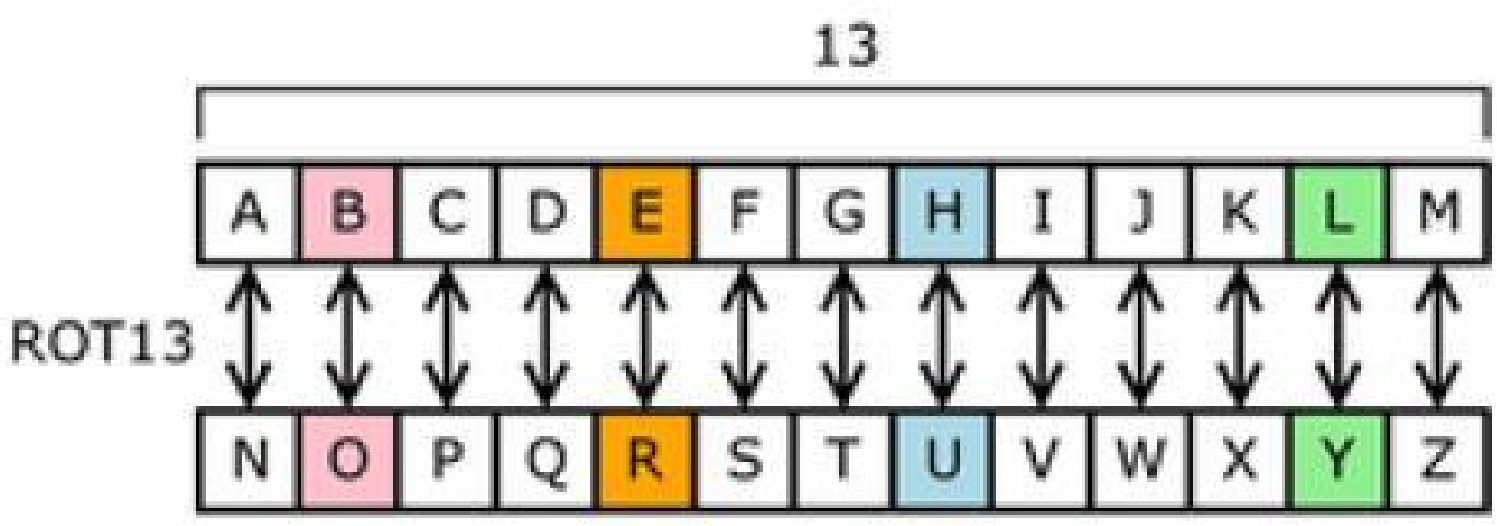
- Used by Caesar to communicate with his generals.
- Each letter is shifted by a constant ($= 3$) position in the alphabet.



  E.g., LUCKNOW $\rightarrow$ OXFNQRZ
- Shift cipher
- # of possibilities $= 26$.
- On average, a plaintext will be computed after trying 13 decryption rules.

Shift Cipher

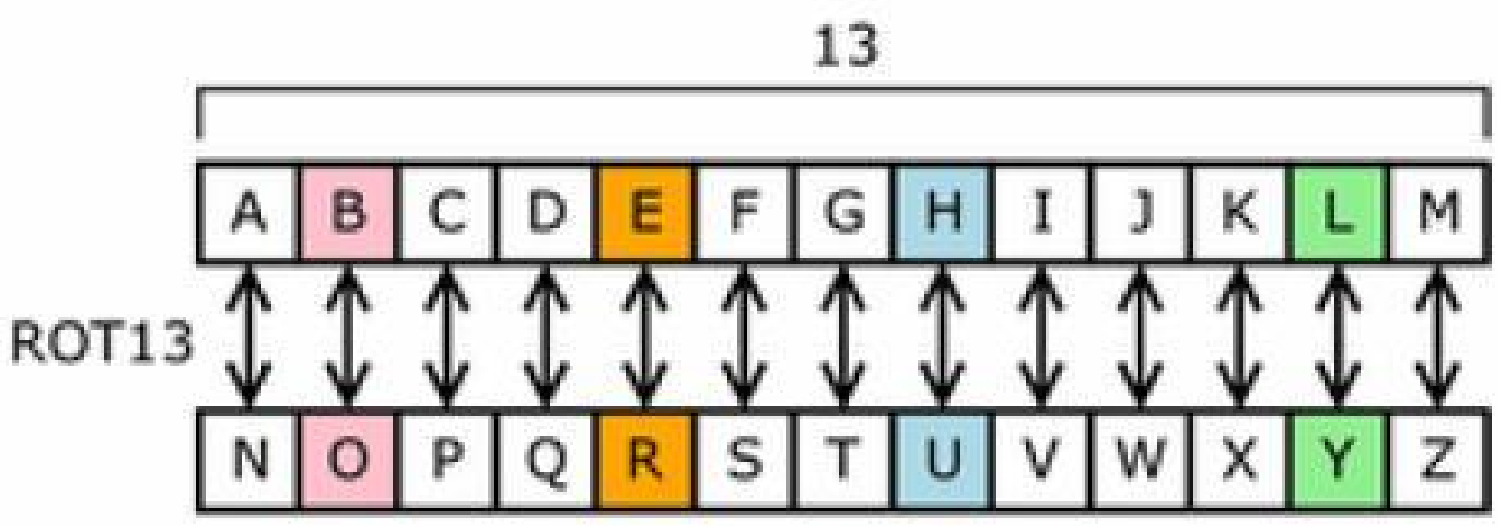
Shift = 13



TECHNOLOGY →

Shift Cipher

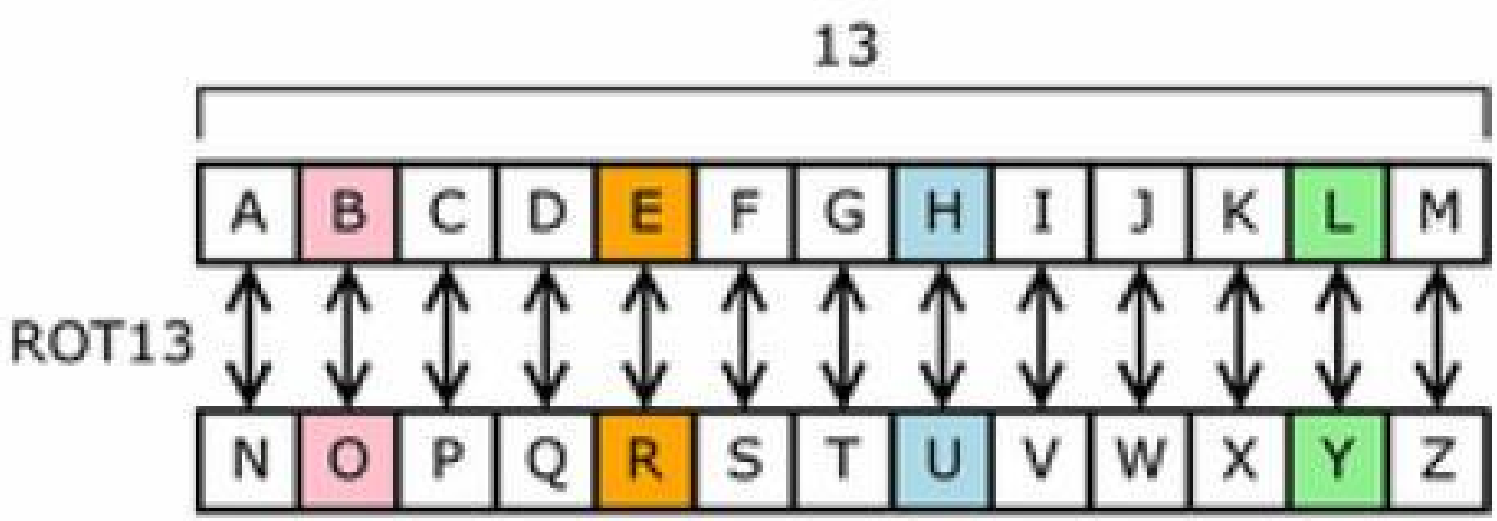
Shift = 13



TECHNOLOGY → GRPUABYBTL

Shift Cipher

Shift = 13



TECHNOLOGY → GRPUABYBTL

Exercise

Ciphertext : TYECZOFNETZY EZ NCJAEZRCLASJ. Find the shift and the plaintext.

Affine Cipher

- An affine cipher is a simple substitution where

$$c_i \equiv (ap_i + b) \ mod \ 26.$$

Affine Cipher

- An affine cipher is a simple substitution where

$$c_i \equiv (ap_i + b) \ mod \ 26.$$

- What is the key-space of this cipher?

Affine Cipher

- An affine cipher is a simple substitution where

$$c_i \equiv (ap_i + b) \; mod \; 26.$$

- What is the key-space of this cipher?

$$26\phi(26)$$

Exercises

Exercise

1. *Evaluate the following:*
   (a) $7503 \mod 81$
   (b) $-7503 \mod 81$

Exercises

Exercise

1. *Evaluate the following:*
   (a) $7503 \mod 81$
   (b) $-7503 \mod 81$
2. *If an encryption function e_K is identical to the decryption function d_K, then the key K is said to be an* ***involutory key****. Find all the involutory keys in the Shift Cipher over $\mathbb{Z}_{26}$.*

Exercises

Exercise

1. *Evaluate the following:*
   (a) $7503 \mod 81$
   (b) $-7503 \mod 81$
2. *If an encryption function e_K is identical to the decryption function d_K, then the key K is said to be an **involutory key**. Find all the involutory keys in the Shift Cipher over $\mathbb{Z}_{26}$.*
3. *Determine the **number of keys** in an Affine Cipher over $\mathbb{Z}_{100}$.*

Exercises

Exercise

1. *Evaluate the following:*
   (a) $7503 \mod 81$
   (b) $-7503 \mod 81$
2. *If an encryption function e_K is identical to the decryption function d_K, then the key K is said to be an **involutory key**. Find all the involutory keys in the Shift Cipher over $\mathbb{Z}_{26}$.*
3. *Determine the **number of keys** in an Affine Cipher over $\mathbb{Z}_{100}$.*
4. *List all the **invertible elements** in $\mathbb{Z}_{35}$.*

Mono-alphabetic Cipher

- Each letter is replaced with another letter, according to a fixed substitution

Mono-alphabetic Cipher

- Each letter is replaced with another letter, according to a fixed substitution

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

HELLO WORLD →

Mono-alphabetic Cipher

- Each letter is replaced with another letter, according to a fixed substitution

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

HELLO WORLD → EZIIP MPWIU
Number of possible keys (Key space):

Mono-alphabetic Cipher

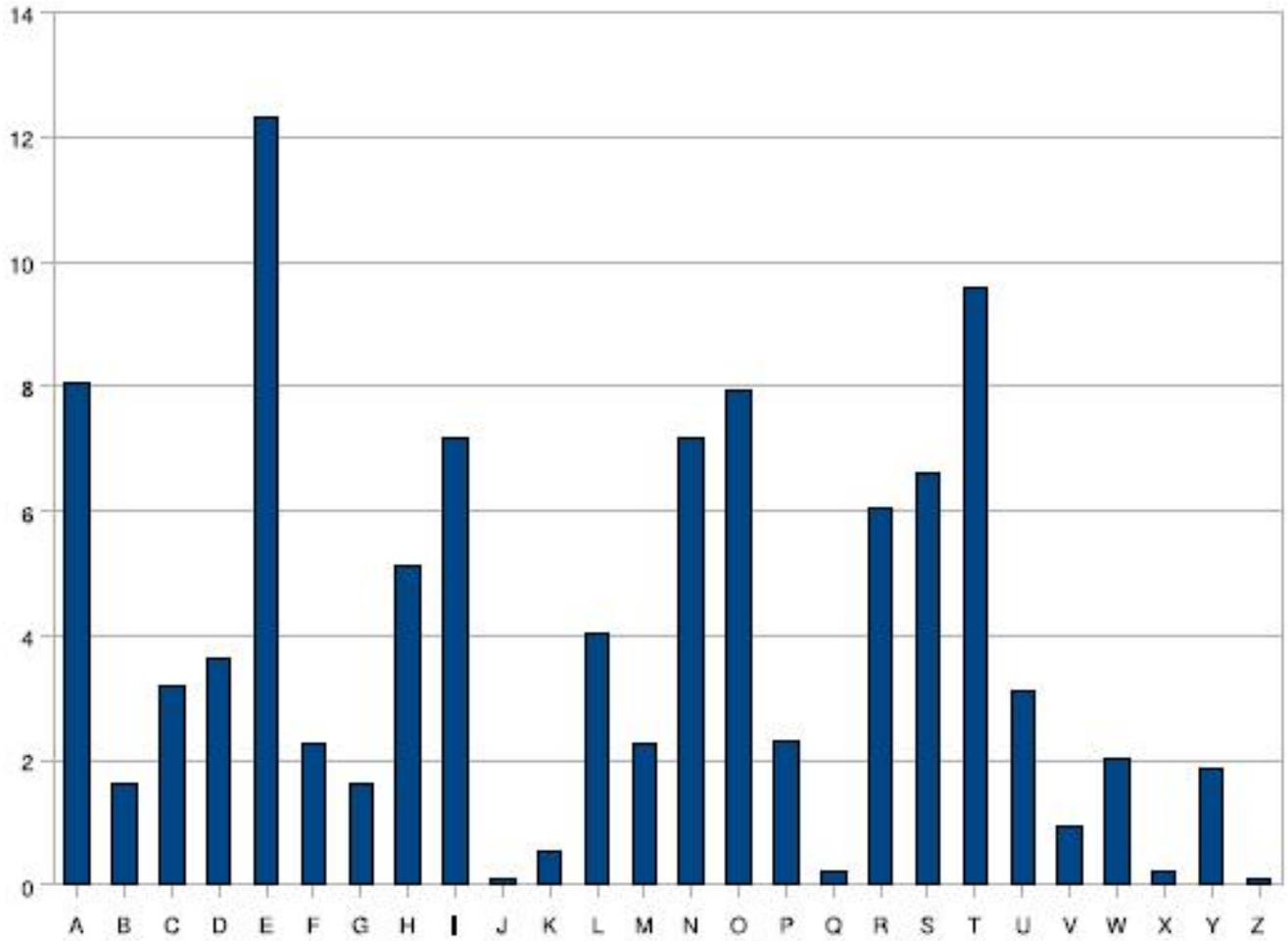
- Each letter is replaced with another letter, according to a fixed substitution

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

HELLO WORLD → EZIIP MPWIU
Number of possible keys (Key space): $26!$

Mono-alphabetic Cipher

Frequency Analysis



Mono-alphabetic Cipher

Frequency Analysis

E	12.7%	D	4.2%	P	1.9%
T	9.0%	L	4.0%	B	1.5%
A	8.2%	U	2.8%	V	1.0%
O	7.5%	C	2.8%	K	0.8%
I	7.0%	M	2.4%	Q	0.1%
N	6.7%	W	2.4%	X	0.1%
S	6.3%	F	2.2%	J	0.1%
H	6.1%	G	2.0%	Z	0.1%
R	6.0%	Y	2.0%		

Mono-alphabetic Cipher

Frequency Analysis

digram	*frequency*	*digram*	*frequency*	*digram*	*frequency*	*digram*	*frequency*
th	3.15	to	1.11	sa	0.75	ma	0.56
he	2.51	nt	1.10	hi	0.72	ta	0.56
an	1.72	ed	1.07	le	0.72	ce	0.55
in	1.69	is	1.06	so	0.71	ic	0.55
er	1.54	ar	1.01	as	0.67	ll	0.55
re	1.48	ou	0.96	no	0.65	na	0.54
es	1.45	te	0.94	ne	0.64	ro	0.54
on	1.45	of	0.94	ec	0.64	ot	0.53
ea	1.31	it	0.88	io	0.63	tt	0.53
ti	1.28	ha	0.84	rt	0.63	ve	0.53
at	1.24	se	0.84	co	0.59	ns	0.51
st	1.21	et	0.80	be	0.58	ur	0.49
en	1.20	al	0.77	di	0.57	me	0.48
nd	1.18	ri	0.77	li	0.57	wh	0.48
or	1.13	ng	0.75	ra	0.57	ly	0.47

Mono-alphabetic Cipher

Frequency Analysis

digram	*frequency*	*digram*	*frequency*	*digram*	*frequency*	*digram*	*frequency*
th	3.15	to	1.11	sa	0.75	ma	0.56
he	2.51	nt	1.10	hi	0.72	ta	0.56
an	1.72	ed	1.07	le	0.72	ce	0.55
in	1.69	is	1.06	so	0.71	ic	0.55
er	1.54	ar	1.01	as	0.67	ll	0.55
re	1.48	ou	0.96	no	0.65	na	0.54
es	1.45	te	0.94	ne	0.64	ro	0.54
on	1.45	of	0.94	ec	0.64	ot	0.53
ea	1.31	it	0.88	io	0.63	tt	0.53
ti	1.28	ha	0.84	rt	0.63	ve	0.53
at	1.24	se	0.84	co	0.59	ns	0.51
st	1.21	et	0.80	be	0.58	ur	0.49
en	1.20	al	0.77	di	0.57	me	0.48
nd	1.18	ri	0.77	li	0.57	wh	0.48
or	1.13	ng	0.75	ra	0.57	ly	0.47

Trigram: the, and, ent, ion, tio, for, nde, . . .

Extension of Mono-alphabetic Cipher

There are three ways to obfuscate the letter frequency:

- **homophone cipher**

Example

Beale cipher – *The oldest known usage in 1401*

Extension of Mono-alphabetic Cipher

There are three ways to obfuscate the letter frequency:

- **homophone cipher**

Example

Beale cipher – *The oldest known usage in 1401*

- **polyalphabetic cipher**

Example

Vigenére Ciphe, Enigma – *The oldest known usage in 1568*

Extension of Mono-alphabetic Cipher

There are three ways to obfuscate the letter frequency:

- **homophone cipher**

Example

Beale cipher – *The oldest known usage in 1401*

- **polyalphabetic cipher**

Example

Vigenére Ciphe, Enigma – *The oldest known usage in 1568*

- **polygraphic cipher**

Example

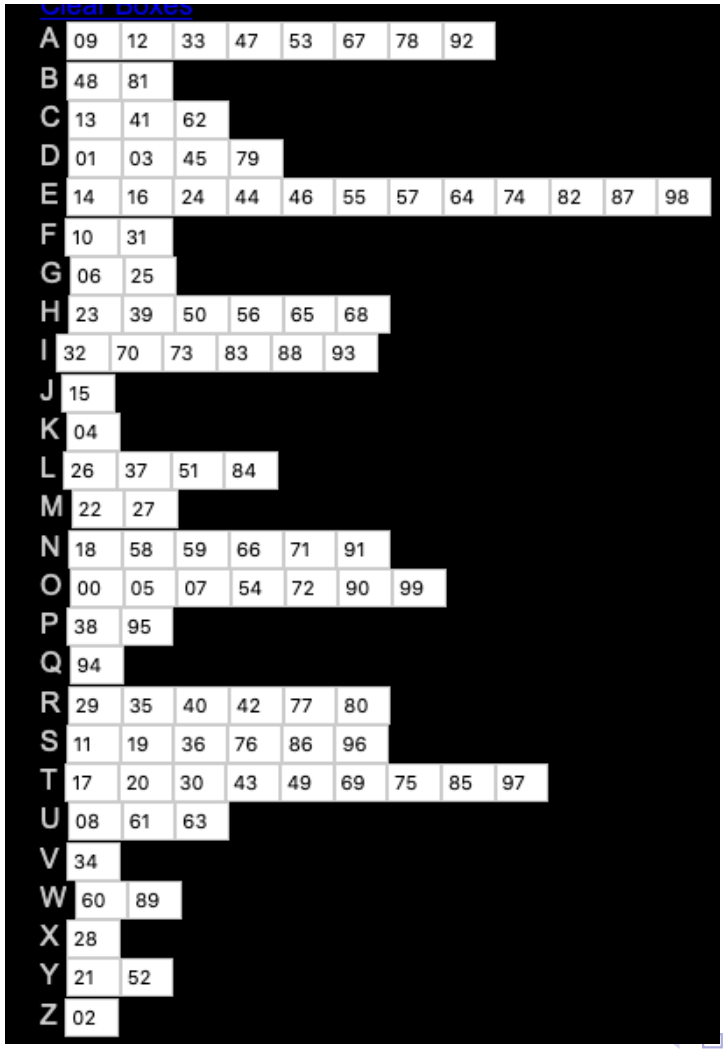
Playfair – *The oldest known usage in 1854*

Homophone Cipher

- The Homophonic Substitution Cipher involves replacing each letter with a variety of substitutes, the number of potential substitutes being proportional to the frequency of the letter.

Homophone Cipher

- The Homophonic Substitution Cipher involves replacing each letter with a variety of substitutes, the number of potential substitutes being proportional to the frequency of the letter.



Homophone Cipher

Exercise

Encrypt the plaintext: Information Systems Security

Homophone Cipher

Exercise

Encrypt the plaintext: Information Systems Security

Homophonic Cipher

Plaintext
Information System Security

Ciphertext
73 91 31 05 35 27 92 69 83 05 91 86 21 19 85 64 22 96 98 41 08 80 93 20 52

Polygraphic Cipher

- A polygraphic cipher is using substitution of a group of characters in the plaintext alphabet, known as “*poligraph*".

Playfair Cipher

- First choose an encryption key, say, POINTS.
- Enter the letters of the key in the cells of a 5×5 matrix in a left to right fashion starting with the first cell at the top-left corner.
- Fill the rest of the cells of the matrix with the remaining letters in alphabetic order.
- The letters I and J are assigned the same cell.

Polygraphic Cipher

Playfair Cipher

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

Polygraphic Cipher

Playfair Cipher

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

UNIVERSITY →

Polygraphic Cipher

Playfair Cipher

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

UNIVERSITY → RTPXHLBPNZ

Polygraphic Cipher

Playfair Cipher

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

UNIVERSITY → RTPXHLBPNZ

SAG →

Polygraphic Cipher

Playfair Cipher

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

UNIVERSITY → RTPXHLBPNZ

SAG →SAGZ →

Polygraphic Cipher

Playfair Cipher

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

UNIVERSITY → RTPXHLBPNZ

SAG →SAGZ → ABKX

Poly-alphabetic Cipher

Vigenére Cipher

- A key of the form $K = (k_o, k_1, \cdots, k_{n-1})$, where each $k_i \in \{0, 1, \cdots, 25\}$, is used to encipher the plaintext.
- Each k_i represents a particular shift of the alphabet.
- To encrypt a message

$$C_i \equiv (P_i + k_{i \bmod n}) \bmod 26$$

- To decrypt

$$P_i \equiv (C_i - k_{i \bmod n}) \bmod 26$$

Exercise

Find the key space of Vigenére Cipher when the length of keyword n

विद्या ददाति विनयं विनयाद् याति पात्रताम्

Poly-alphabetic 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	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

Poly-alphabetic Cipher

Vigenére Cipher

- **Plaintext:** HPUNIVERSITY
- **Keyword:** UIT
- **Ciphertext:**

Poly-alphabetic Cipher

Vigenére Cipher

- **Plaintext:** HPUNIVERSITY
- **Keyword:** UIT
- **Ciphertext:**

BXNHQOYZLCBR

Analysis

- A poly-alphabetic substitution cipher uses multiple simple substitutions to encrypt a message
- A polyalphabetic substitution does not preserve plaintext letter frequencies to the same degree as a mono-alphabetic substitution.
- However, if the length keyword is known and the message is long enough, we can transform this into class of simple substitution.

Analysis

How to determine the length of an unknown keyword

- **Kasiski Test**
  - It relies on the occasional coincidental alignment of letter groups in plaintext with the keyword.
  - It was described by Friedrich Kasiski in 1863; however, it was apparently discovered earlier, around 1854, by Charles Babbage.
  - We find repeated letter groups in the ciphertext arid tabulate the separations between them.
  - The gcd of these separations gives a possible length for the keyword.

Analysis

How to determine the length of an unknown keyword

- **Index of Coincidence**
  - The index of coincidence I is defined to be the probability that two randomly selected letters in the ciphertext represent the same plaintext symbol.
  - This concept was defined by William Friedman in 1920.
  - The index of coincidence of English text ≈ 0.065.
  - I for a random text ≈ 0.03846.
  - For any English ciphertext the index of coincidence I must satisfy $0.03846 \leq I \leq 0.065$.

Poly-alphabetic Cipher

Hill Cipher[1]

- Encryption key,

$$K = \begin{pmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{32} & k_{33} \end{pmatrix}$$

[1] Hill cipher was developed by **Lester S. Hill**, an American mathematician.

Poly-alphabetic Cipher

Hill Cipher[1]

- Encryption key,

$$K = \begin{pmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{32} & k_{33} \end{pmatrix}$$

- The plaintext letters p_1, p_2 & p_3 encrypted into ciphertext letters c_1, c_2 & c_3 by

$$\begin{pmatrix} c_1 \\ c_2 \\ c_3 \end{pmatrix} = \begin{pmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{32} & k_{33} \end{pmatrix} \begin{pmatrix} p_1 \\ p_2 \\ p_3 \end{pmatrix}$$

[1] Hill cipher was developed by **Lester S. Hill**, an American mathematician.

Exercises

Exercise

1. *Let p be prime. Find the number of 3×3 invertible matrices over $\mathbb{Z}_p$.*
2. *Find the number of $n \times n$ invertible matrices over $\mathbb{Z}_p$.*
3. *Find the number of $n \times n$ invertible matrices over $\mathbb{Z}_{p^\alpha}$*
4. *Find the number of $n \times n$ invertible matrices over $\mathbb{Z}_m$*

Cryptography During The French and American Wars in Vietnam

CRYPTOGRAPHY DURING THE FRENCH AND AMERICAN WARS IN VIETNAM

PHAN DƯƠNG HIỆU AND NEAL KOBLITZ

ABSTRACT. After Vietnam's Declaration of Independence on 2 September 1945, the country had to suffer through two long, brutal wars, first against the French and then against the Americans, before finally in 1975 becoming a unified country free of colonial domination. Our purpose is to examine the role of cryptography in those two wars. Despite the far greater technological resources of their opponents, the communications intelligence specialists of the Việt Minh, the National Liberation Front, and the Democratic Republic of Vietnam had considerable success in both protecting Vietnamese communications and acquiring tactical and strategic secrets from the enemy. Perhaps surprisingly, in both wars there was a balance between the sides. Generally speaking, cryptographic knowledge and protocol design were at a high level at the central commands, but deployment for tactical communications in the field was difficult, and there were many failures on all sides.

http://eprint.iacr.org/2016/1136.pdf

Classical Ciphers

- These ciphers are too weak nowadays, too easy to break, especially with computers.
- However, these simple ciphers give a good illustration of several of the important ideas of the cryptography and cryptanalysis.
- Moreover, most of them can be very useful in combination with more modern cipher – to add a new level of security.

Block Cipher

Block Cipher

- Avoid transport & storage of huge table
- Introduce computation rule to compute table elements:

$$T[X] = f_{key}(X)$$

- Design “good" rule f:

Block Cipher

- Avoid transport & storage of huge table
- Introduce computation rule to compute table elements:

$$T[X] = f_{key}(X)$$

- Design “good" rule f:
  - Secure
  - Efficient

Permutation on Block of Characters

Example

AAAA	AAAB	AAAC	$\cdots$	ZZZZ
QAQZ	WIJT	ENTO	$\cdots$	MIHB

Permutation on Block of Characters

Example

AAAA	AAAB	AAAC	$\cdots$	ZZZZ
QAQZ	WIJT	ENTO	$\cdots$	MIHB

- '*code book*'

Permutation on Block of Characters

Example

AAAA	AAAB	AAAC	$\cdots$	ZZZZ
QAQZ	WIJT	ENTO	$\cdots$	MIHB

- '*code book*'
- If blocks are large enough, then frequency analysis becomes impossible (infeasible).

The End

Thanks a lot for your attention!