CS 413
Information Security

Course Instructor

Naushad Siddiqui

Head of IT Audit, Sui Southern Gas Company

Visiting Faculty, NED University

Director & Faculty Member, ISACA Karachi

CS413 Information Security

Fall 2020

Week 05

Agenda

- Substitution & Transposition Cipher
- Monoalphabetic vs Polyalphabetic Cipher
- Stream and Block Cipher
- Vigenere Cipher
- Breaking the Vigenere Cipher

Substitution & Transposition Cipher

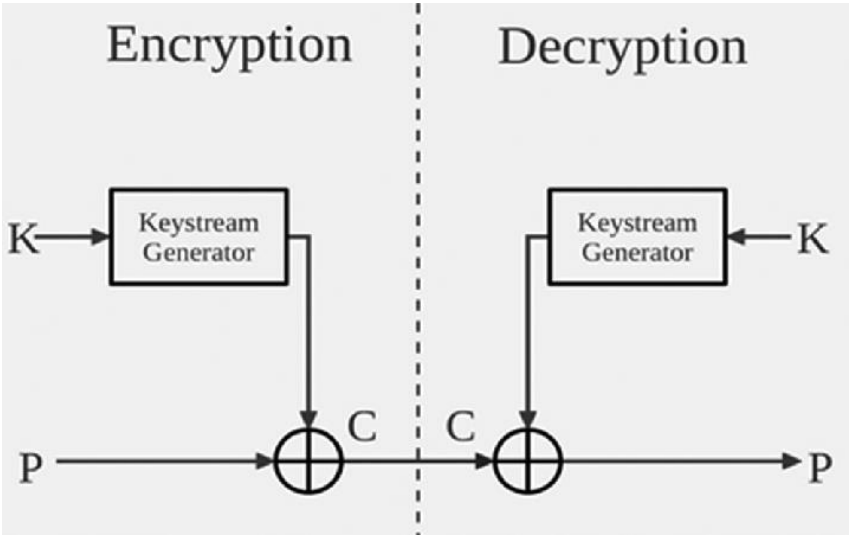
- **Substitution Cipher**
  - It replaces one symbol of plain text with another.
  - ‘units’ of plaintext are replaced with ciphertext, according to a fixed system
  - ‘units’ may be single letters (the most common), pairs of letters, triplets of letters, mixtures of the above, and so forth
  - It could be *Mono-alphabetic Cipher* or *Ploy-alphabetic Cipher*
- **Transposition Cipher**
  - It does not substitute one symbol for another, instead it changes the position / location of the symbols.
  - It actually REORDERS symbol in the plain text to generate cipher-text
  - Plaintext characters are shifted in some regular pattern to form ciphertext

Monoalphabetic vs Polyalphabetic Cipher

- **Mono-alphabetic Cipher**
  - each occurrence of a character in the plaintext have same substitution in the cipher-text
  - the relationship between a symbol in plaintext to a symbol in cipher-text is ONE-to-ONE
  - Examples: Caeser Cipher
  - Main weaknesses of monoalphabetic substitution ciphers
    - each letter in the ciphertext corresponds to only one letter in the plaintext letter
    - frequency of characters in the cipher-text is not changed
- **Poly-alphabetic Cipher**
  - In this cipher, each occurrence of a character in the plaintext may have different substitution in the cipher-text
  - the relationship between a symbol in plaintext to a symbol in cipher-text is ONE-to-MANY
  - Examples: Playfair Cipher

Stream and Block Cipher

- **Stream Cipher**
  - Encryption and Decryption are done on one symbol (a character, a bit or a unit) at a time
  - In this, we have a Plaintext Stream, a Ciphertext Stream and a Key Stream



  - Examples:
    - Caeser Cipher
    - Playfair Cipher can be treated as Stream Cipher for the whole plaintext, where the UNIT is the pair of plaintext

Stream and Block Cipher

- **Block Cipher**
  - A block cipher is an encryption method that applies a deterministic algorithm along with a symmetric key to encrypt a block of text, rather than encrypting one bit at a time
  - For example, a common block cipher, AES, encrypts 128 bit blocks with a key of predetermined length: 128, 192, or 256 bits.
  - A single key is used to encrypt the whole block
  - Examples:
    - Playfair Cipher, size of the block is ‘2’
    - Hill Cipher

Vigenere Cipher

Vigenere Cipher

Polyalphabetic Substitution Ciphers

- Idea for a stronger cipher (1460's by Alberti)
  - Use more than one substitutions, and switch between them when encrypting different letters
  - As result, frequencies of letters in ciphertext are similar
- Developed into an easy-to-use cipher by Vigenère (published in 1586)

Vigenere Cipher

Vigenere Ciphers

- The Vigenere cipher is probably the best-known example of a polyalphabetic cipher, though it is a simplified special case.
- It was used in the American civil war and was once believed to be unbreakable.
- A Vigenere cipher uses a different strategy to create the key stream. The key stream is a repetition of an initial secret key stream of length ‘m’, where we have 1 <= m <= 26.
- The Vigenere cipher is a method of encrypting alphabetic text by using a series of different Caesar ciphers based on the letters of a keyword.

Vigenere Cipher

Concept

Plain Text	$P = P_1P_2P_3 \ldots$
Cipher Text	$C = C_1C_2C_3 \ldots$
Key Stream	K = [(*k1, k2, …, km*), (*k1, k2, …, km*), ….]
Encryption	$C_i = P_i + k_i$
Decryption	$P_i = C_i - k_i$

Suppose m=6 and the key word is CIPHER,
this correspond to the numeric equivalent K = { 2, 8, 15, 7, 4, 17 }

Plain Text : This Crypto System is not Secure

Cipher Text Message
VPXZGI AXIVWP UBTTMJ PWIZIT WZT

Vigenere Cipher

Mathematical Representation

Recall that letters as numbers: [A=0, B=1, C=2, …, Z=25]

Number Theory Notation: $Z_n = \{0, 1, \ldots, n-1\}$

Definition:

Given m, a positive integer, $P = C = (Z_{26})^n$, and $K = (k_1, k_2, \ldots, k_m)$ a key, we define:

Encryption:

$e_k(p_1, p_2 \ldots p_m) = (p_1+k_1, p_2+k_2 \ldots p_m+k_m) \pmod{26}$

Decryption:

$d_k(c_1, c_2 \ldots c_m) = (c_1-k_1, c_2-k_2 \ldots c_m-k_m) \pmod{26}$

Example:

Plaintext: C R Y P T O G R A P H Y

Key: L U C K

Ciphertext: N L A Z E I I B L J J I

Vigenere Cipher

Example

We can encrypt the message **"She is listening"** using the 6-character keyword **"PASCAL"**. The initial key stream is **(15,0,18,2,0,11)**

The key stream is the repetition of this initial key stream (as many times as needed)

Use encryption algo: $C_i = P_i + k_i$

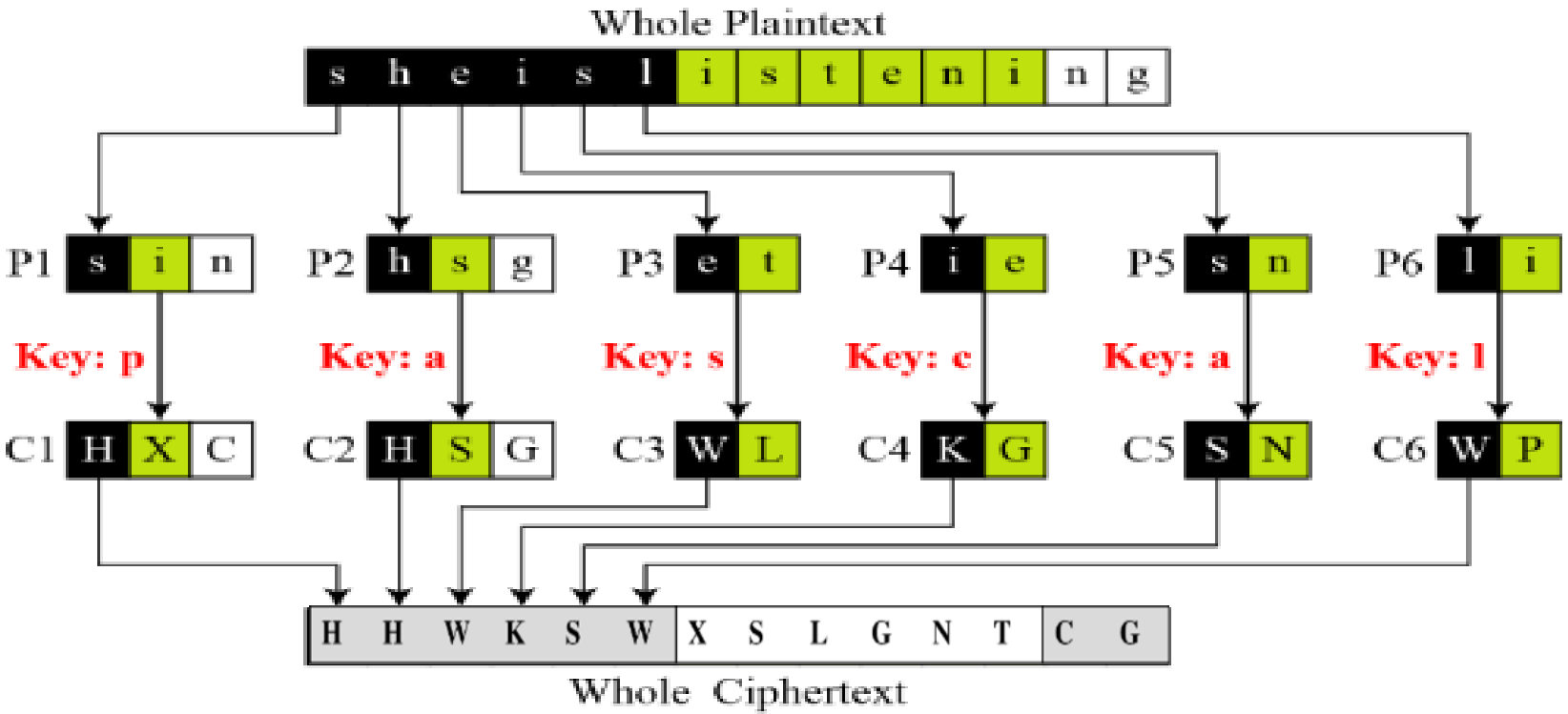
Plaintext:	s	h	e	i	s	l	i	s	t	e	n	i	n	g
P's values:	18	07	04	08	18	11	08	18	19	04	13	08	13	06
Key stream:	*15*	*00*	*18*	*02*	*00*	*11*	*15*	*00*	*18*	*02*	*00*	*11*	*15*	*00*
C's values:	**07**	**07**	**22**	**10**	**18**	**22**	**23**	**18**	**11**	**6**	**13**	**19**	**02**	**06**
Ciphertext:	**H**	**H**	**W**	**K**	**S**	**W**	**X**	**S**	**L**	**G**	**N**	**T**	**C**	**G**

Note: *The Vigenere key stream does not depend on the plaintext characters. It depends only on the position of the character in the plain text.*

Vigenere Cipher

***Example** (…cont…)*

Vigenere cipher can be seen as combinations of ‘m’ additive ciphers.



Vigenere Cipher

Vigenere Table

- Another way to look at Vigenere ciphers is through what is called a ***Vigenere Tableau***, ***Vigenere Table*** or ***Vigenere Square***.
- The table consists of the alphabets written out 26 times in different rows, each alphabet shifted cyclically to the left compared to the previous alphabet, corresponding to the 26 possible Caesar Ciphers.
- The first row of this table has the 26 English letters.
- Starting with the second row, each row has the letters shifted to the left one position in a cyclic way.
- For example, when B is shifted to the first position on the second row, the letter A moves to the end.
- The first column contains the characters to be used by the key.

Vigenere Cipher

Vigenere Table

	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

Vigenere Cipher

Vigenere Table - example

To find the cipher text for the plaintext **'she is listening'** using the word **'PASCAL'** as the key

s	h	e	i	s	l	i	s	t	e	n	i	n	g
P	A	S	C	A	L	P	A	S	C	A	L	P	A

- we can find **"s"** in the first row**,** **"p"** in the first column, the cross section is the cross section is the cipher text character **"H"**
- we can find **"h"** in the first row, **"A"** in the first column, the cross section is the cross section is the cipher text character **"H"**
- and so on, finally getting this:

H	H	W	K	S	W	X	S	L	G	N	T	C	G

	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

Vigenere Cipher

Vigenere Table – Encryption Example

“TO BE OR NOT TO BE THAT IS THE QUESTION”

Use Vigenere table method to encrypt plain text to cipher text, with key word RELATIONS

Plaintext:	TOBEORNOT TOBETHATI STHEQUEST ION
Keyword:	RELATIONS RELATIONS RELATIONS REL
Ciphertext:	KSMEHZBBL KSMEMPOGA JXSEJCSFL ZSY

Vigenere Cipher

Vigenere Table – Decryption Example

Decryption is performed by going to the row in the table corresponding to the KEY, finding the position of the ciphertext letter in this row, and then using the column's label as the plaintext.

"TO BE OR NOT TO BE THAT IS THE QUESTION"

Use Vigenere table method to decrypt cipher text to plain text, with key word RELATIONS

Keyword:	RELATIONS RELATIONS RELATIONS REL
Ciphertext:	KSMEHZBBL KSMEMPOGA JXSEJCSFL ZSY
Plaintext:	TOBEORNOT TOBETHATI STHEQUEST ION

Breaking the Vigenere Cipher

Breaking the Vigenere Cipher

Security of Vigenere Cipher

- Vigenere masks the frequency with which a character appears in a language

  one letter in the ciphertext corresponds to multiple letters in the plaintext

- Makes the use of frequency analysis more difficult.
- Any message encrypted by a Vigenere cipher is a collection of as *many shift ciphers* as there are letters in the key.

Breaking the Vigenere Cipher

Cryptanalysis

- Vigenere-like substitution ciphers were regarded by many as practically unbreakable for 300 years.
- In 1863, major **Kasiski** proposed a method for breaking a Vigenere cipher that consisted of finding the length of the keyword and then dividing the message into that many simple substitution cryptograms.
- Frequency analysis could then be used to solve the resulting simple substitutions.
- Checking which of the 26 possible shifts give rises to the correct decryption.
- It can be done by checking how well the resulting frequency distribution matches that of the underling language.

Breaking the Vigenere Cipher

Unbreakable Code

- The strength of the Vigenère Cipher is that the same letter can be encrypted in different ways.
- **For example, if the keyword is KING, then every plaintext letter can be encrypted in 4 ways, because the keyword contains 4 letters.**
- Each letter of the keyword defines a different cipher alphabet in the Vigenère Square.
- Whole words will be enciphered in different ways - the word 'the' could be enciphered as DPR, BUK, GNO and ZRM depending on its position relative to the keyword.
- Although this makes cryptanalysis difficult, it is not impossible.

Breaking the Vigenere Cipher

Unbreakable Code

- If there are only four ways to encipher the word 'the', and the original message contains several uses of the word 'the', then it is inevitable that some of the four possible encipherments will be repeated in the ciphertext.
- This is demonstrated in the following example, in which the line "The Sun and the Man in the Moon", has been enciphered using the Vigenere cipher and the keyword KING.

KINGKINGKINGKINGKINGKING	keyword
THESUNANDTHEMANINTHEMOON	plaintext
DPRYEVNTNBUKWIAOXBUKWWBT	cipher

The letters BUK repeat after 8 letters.

This suggests that the number of letters in the keyword is a factor of 8. So, the keyword has 2, 4, or 8 letters.

Breaking the Vigenere Cipher

Breaking the Code

- The word 'the' is enciphered as DPR in the first instance, and then as BUK on the second and third occasions.
- The reason for the repetition of BUK is that the second 'the' is displaced by 8 letters with respect to the third 'the', and 8 is a multiple of the length of the keyword.
- In other words, the second 'the' was enciphered according to its relationship to the keyword, and by the time we reach the third 'the', the keyword has cycled round exactly twice, to repeat the relationship.

Breaking the Vigenere Cipher

Breaking the Code

- Babbage's vital breakthrough was to realize that repetitions in the ciphertext indicated repetitions in the plaintext and that the space between such repetitions hinted at the length of the keyword.
- Once the length of the keyword is determined, the message can be broken up into the corresponding number of messages, each one is a caesar shifted cipher, and amenable to frequency analysis.

- This is how Babbage cracked the Vigènere Cipher.

End of Week 05