Classical cryptography

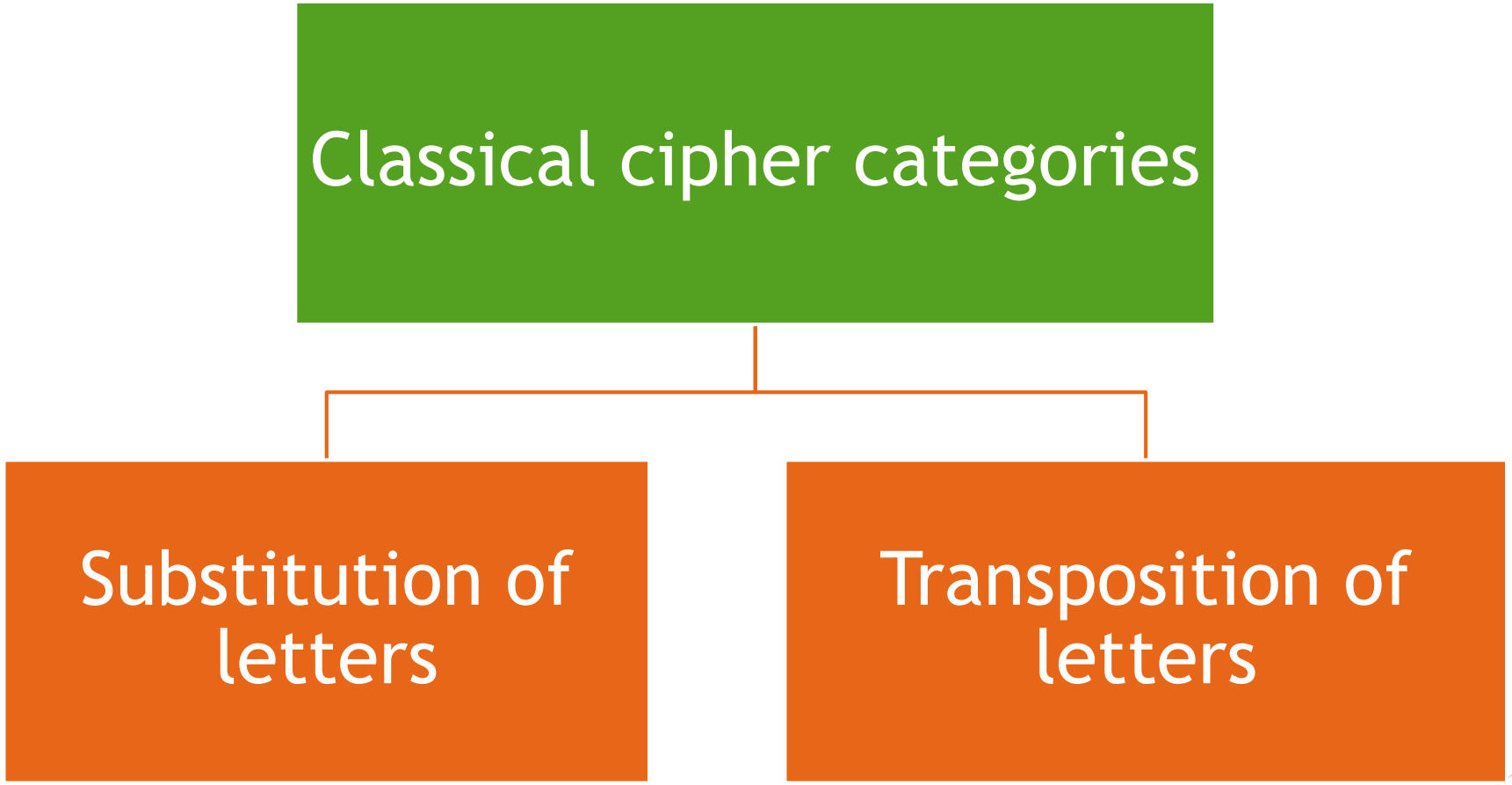
Pr. Noureddine Chikouche
noureddine.chikouche@univ-msila.dz
https://sites.google.com/view/chikouchenoureddine

Course outline

- Classic encryption categories
- Frequency analysis
- Shift Cipher
- Vigenère Cipher
- Affine Cipher
- Transposition Cipher
- Assyrian cipher

- Classical cryptography…

Classic encryption categories



Classic encryption categories

- **Substitution cipher:**
  - Each character in the plain text is replaced by a character in an encrypted text.
- Monoalphabetic cipher: 1 letter→ 1 single letter.
- Polyalphabetic cipher: 1 letter→ 1 letter among several.
- Polygraphic encryption: n letter →n another letter.
- Examples: shift, Vigenère, affine, Hill, …

Classic encryption categories

- **Transposition cipher:**
  - We encrypt message in swapping the order of the letters of the following plaintext well-defined rules.
  - It consists of changing the positions of the letters.
  - **Examples:** Assyrian technique, rectangular transposition.

Frequency analysis

Frequency analysis is a cryptanalysis technique discovered by Al-Kindi.
Al-Kindi(801-873).

Frequency analysis

- It consists of examining the frequency of letters used in a ciphertext.
- It is the study of the distribution of letters in a text.
- This technique only works well if:
  - the plaintext is long to obtain meaningful averages.
  - Knowing the used language.

Frequency analysis: Principle

- Example: the frequencies of occurrence of letters in the French language:

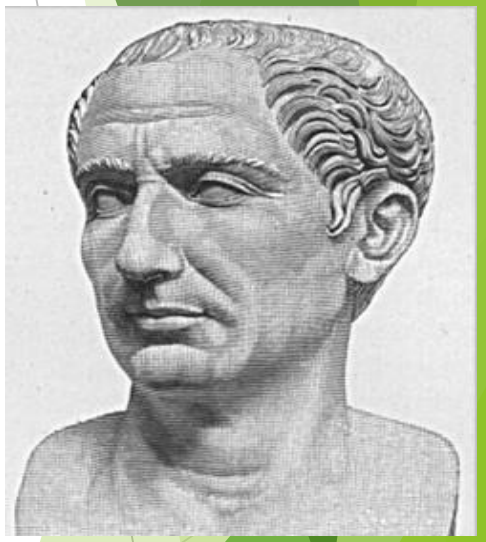
Letter	Frequency %
E	17.76
S	8.23
A	7.68
N	7.61
T	7.30
I	7.23
. . .	

Frequency analysis

- Frequency analysis consists of:
  - identifying the occurrences of letters in the message.
  - Then you just need to proceed by correspondence,
    we will associate the most frequent letter in the ciphertext with the most frequent letter in the language of the reference text.

Shift cipher

- Also called Caesar cipher(50 BC)
- This is the simplest and oldest classical cipher that has ever existed.
- Its principle is a shift of the letters of the alphabet. In the formulas below, x is the index of the letter of the alphabet, k is the shift.
  - k∈ $\mathbb{Z}/26\mathbb{Z}$(is a static integer)
- For encryption, we have the following formula:
  - **$y=E_k(x) = x+k \bmod 26$**
- For decryption, we have the formula:
  - **$x=D_k(y) = y-k \bmod 26$**



Shift cipher

- The 26 letters of the alphabet are numbered from 0 for A to 25 for 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
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

X= CRYPTOGRAPHY

K = D = 3

Shift cipher

Plain text	C	R	Y	P	T	O
Index. Pleantext	2	17	24	15	19	14
Key	D	D	D	D	D	D
Index. Key	3	3	3	3	3	3
Ind.Number	5	20	1	18	22	17
Ciphertext	F	U	B	S	W	R

- Example:
  - $E(2)_k = 2+3 \ \% \ 26 = 5$
  - $D(5)_k = 5-3 \ \% \ 26 = 2$

Shift cipher: Cryptanalysis

❶By finding the value of the offset:

- You just need to test all possible encryption methods until you find the right one. That's what's called a brute force attack, a technique for testing all possible combinations, there are 25 keys are possible.

Shift cipher: Cryptanalysis

❷Frequency analysis:

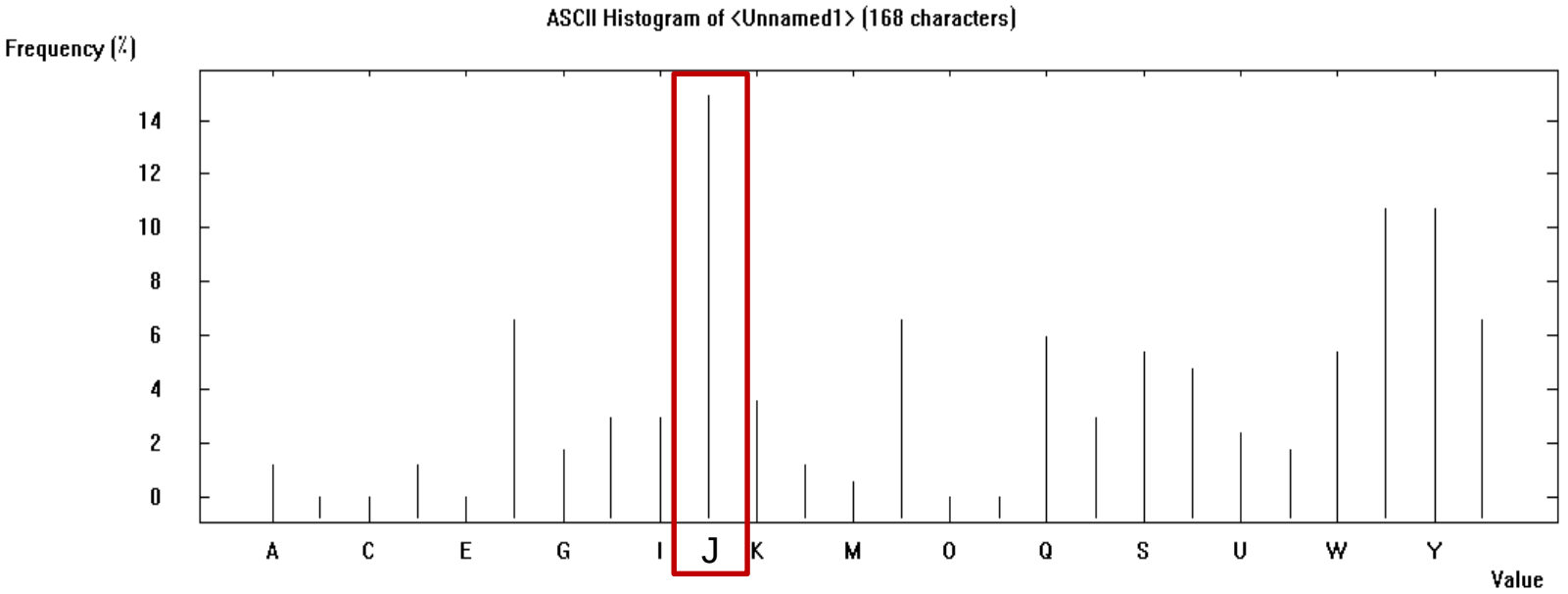
We use the principle of frequency analysis.

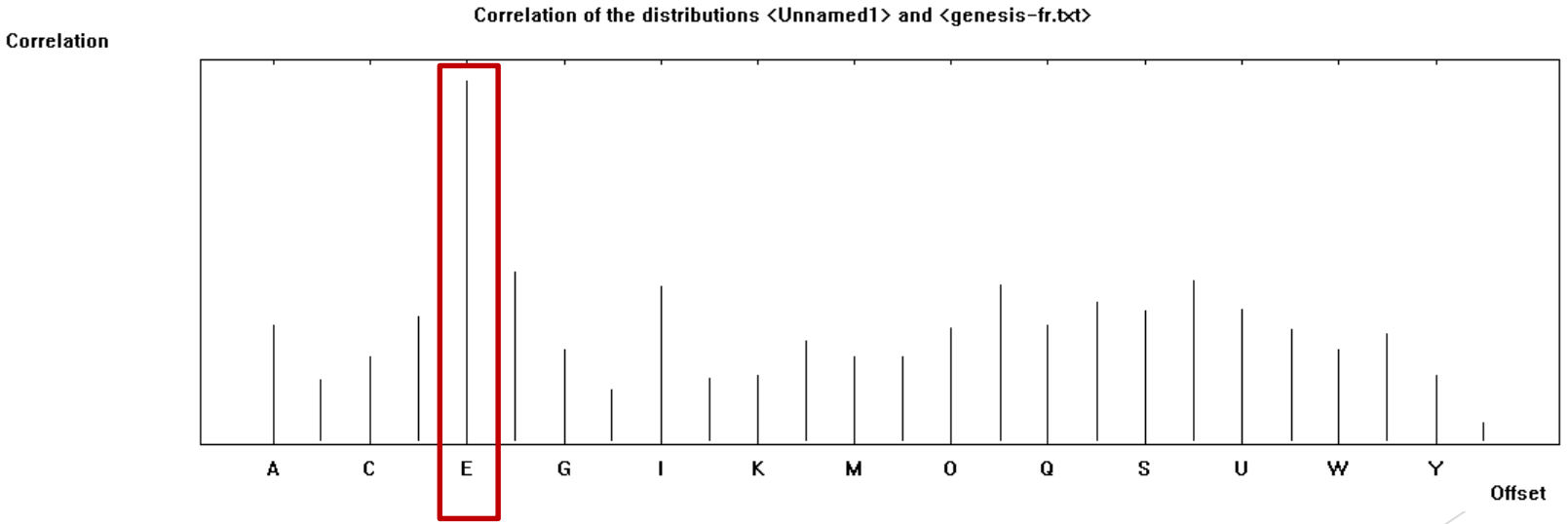
- Example:

QFXZG XYNYZ YNTSR TSTFQ UMFGJ YNVZJ JXYYW JXAZQ

SJWFG QJFQF HWDUY FSFQD XJUTZ WAZVZ JQJRJ XXFLJ

HJIJX INKKJ WJSYJ XQJYY WJX


ASCII Histogram of <Unnamed1> (168 characters)
Frequency (%)
14
12
10
8
6
4
2
0
A C E G I J K M O Q S U W Y
Value


Correlation of the distributions <Unnamed1> and <genesis-fr.txt>
Correlation
A C E G I K M O Q S U W Y
Offset

Shift cipher: Cryptanalysis

- So, J (ciphertext) = E (plaintext)
- E(x) = x + k % 26 => k = E(x) – x % 26
- k = 9 – 4 =5 (F).
- The plain text is:

THE MONOALPHABETICAL SUBSTITUTION IS VERY VULNERABLE TO CRYPTANALYSIS SO THAT THE MESSAGES ARE LONG ENOUGH IT IS ENOUGH TO TAKE ACCOUNT OF THE STATISTICS OF THE OCCURRENCY OF THE DIFFERENT LETTERS

Monoalphabetic substitution is very vulnerable to cryptoanalysis, provided the message is sufficiently long; it suffices to consider the occurrence statistics of the different letters.

Vigenère cipher

- Developed by Blaise de Vigenère (1523, 1596).
- Vigenère cipher of type polyalphabetic.
- This encryption introduces the concept of key.
- A key usually comes in the form of a word or a sentence.
- To encrypt a text, we use a letter from the key for each character to perform the substitution.

Vigenère cipher

- $k = (k_1, k_2, \ldots, k_n)$, $k_i \in \mathbb{Z}/26\mathbb{Z}$k is a set of integers
- For encryption, we have the following formula:
  - $y = E_k(x_1, x_2, \ldots, x_n) = (x_1 + k_1, x_2 + k_2, \ldots, x_n + k_n)$
- For decryption, we have the formula:
  - $x = D_k(y_1, y_2, \ldots, y_n) = (y_1 - k_1, y_2 - k_2, \ldots, y_n - k_n)$
- The operations are carried out in $\mathbb{Z}/26\mathbb{Z}$

Vigenère cipher

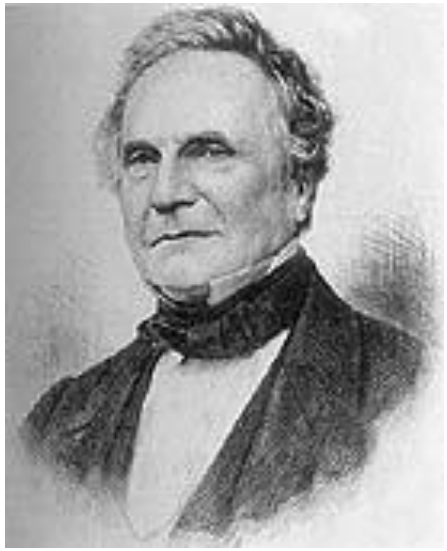
- Plain text: **CHIFFREMENT**
- Key: SECRET =(18, 4, 2, 17, 4, 19)

Plain text	C	H	I	F	F	R	E	M	E	N	T
Index.Plaintxt	2	7	8	5	5	17	4	12	4	13	19
Key	S	E	C	R	E	T	S	E	C	R	E
Index. Key	18	4	2	17	4	19	18	4	2	17	4
Ind.Ciphertext	20	11	10	22	9	10	22	16	6	4	23
Ciphertext	U	L	K	W	J	K	W	Q	G	E	X

- Example:
  - $E(13)_k$=13+17% 26 = 4
  - $D(4)_k$=4 - 17% 26 = -13% 26 = -13 + 26 = 13

Vigenère cipher: Cryptanalysis

- In the 19th century, Charles Babbage succeeded in breaking Vigenère's cryptography.
- He used a technique called "Coincidence index attack"



Vigenère cipher: Cryptanalysis

- Phase1:find the length of the key (n).
  - Stage1: Underline each repetition of 3 or more characters.
  - Stage2: For each repetition, measure the period.
  - Stage3: For each period, decompose into prime factors and see which factor is common to all.

Vigenère cipher: Cryptanalysis

- **Phase2:** find the first letter (i=1) of the keyword.
  - Stage1: perform a frequency analysis only on the characteristics i, N+i, 2N+i, 3N+i,...
  - Stage2: We shift to make it match. (we have the first (i^{th}(letter of the key)
- **Phase 3,4..,i,..**(number of letters in the remaining key): We repeat for the N letters of the keyword.

Vigenère Cryptanalysis: Example Phase1

- KQOWEFVJPUJUUNUKGLMEKJINMWUXFQMKJBGWRLFNFGHUDWUUMBSVLPSNCMUEKQCTESWREEKOYSSIW
  CTUAXYOTAPXPLWPNTCGOJBGFQHTDWXIZAYGFFNSXCSEYNCTSSPN
  TUJNYTGGWZGRWUUNEJUUQEAPYMEKQHUIDUXFPGUYTSMTFFSHNUOCZGMRUWEYTRGKMEEDCTVRECFB
  DJQCUSWVBPNLGOYLSKMTEFVJJTWWMFMWPNMEMTMHRSPXFSSKFFST
  NUOCZGMDOEOYEEKCPJRGPMURSKHFRSEIUEVGOYCWXIZAYGOSAANYDOEOYJLWUNHAMEBFELXYVLWNOJ
  NSIOFRWUCCESWKVIDGMUCGOCRUWGNMAAFFVNSIUDEKQHCEUCPF
  CMPVSUDGAVEMNYMAMVLFMAOYFNTQCUAFVFJNXKLNEIWCWODCCULWRIFTWGMUSWOVMATNYBUHTCOC
  WFYTNMGYTQMKBBNLGFBTWOJFTWGNTEJKNEEDCLDHWTVBUVGFBIJG

Phase 1
Step 1

- UKGLMEKJINMWUXFQMKJBGWRLFNFGHUDWUUMBSVLPSNCMUEKQCTESWREEKOYSSIW
  PNTCGOJBGFQHTDWXIZAYGFFNSXCSEYNCTSSPNTUJNYTGGWZGRWUUNEJUUQEAPYME
  TSMTFFSHNUOCZGMRUWEYTRGKMEEDCTVRECFBDJQCUSWVBPNLGOYLSKMTEFVJJTWW
  MFMWPNMEMTMHRSPXFSSKFFSTNUOCZGMDOEOYEEKCPJRGPMURSKHFRSEIUEVGOYCWXIZAYGOSAANYDO
  EOYJLWUNHAMEBFELXYVLWNOJNSIOFRWUCCESWKVIDGMUCGOCRUWGNMAAFFVNSIUDEKQHCEUCPFCMP
  VSUDGAVEMNYMAMVLFMAOYFNTQCUAFVFJNXKLNEIWCWODCCULWRIFTWGMUSWOVMATNYBUHTCOCWFY
  TNMGYTQMKBBNLGFBTWOJFTWGNTEJKNEEDCLDHWTVBUVGFBIJG

Source:https://www.apprendre-en-ligne.net/crypto/vigenere/decodevig.html

Vigenère Cryptanalysis: Example Phase1

Step 2

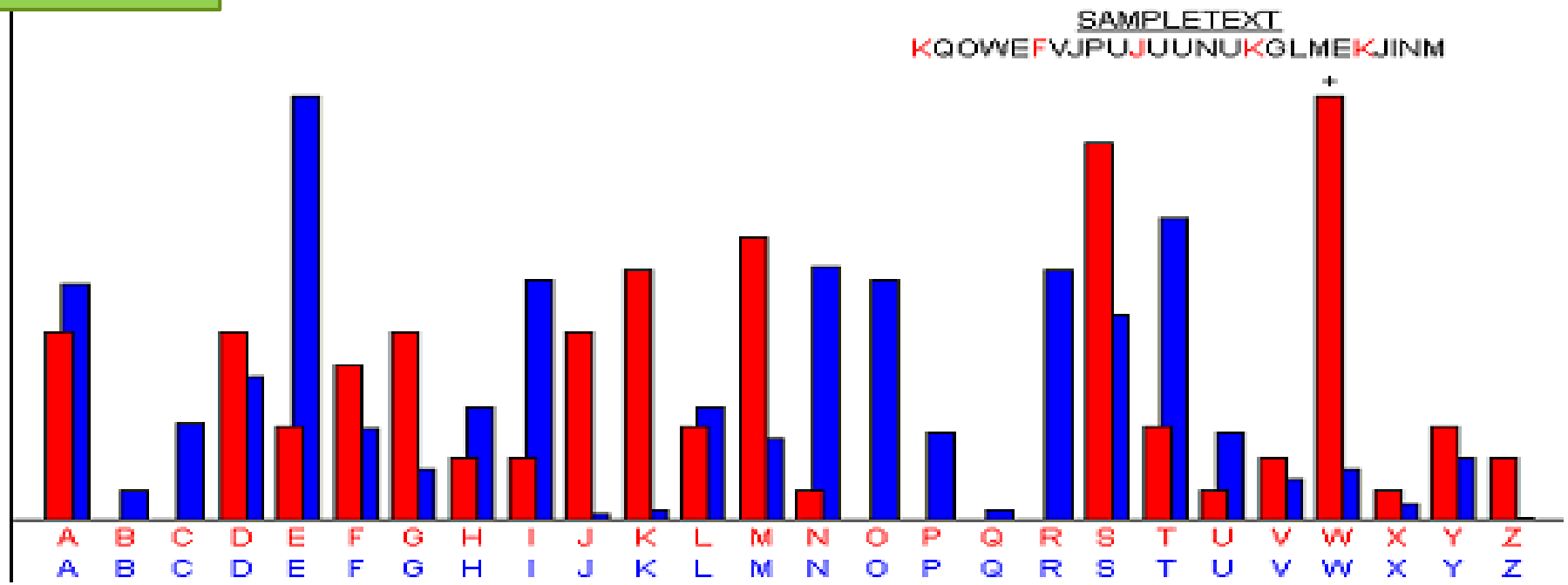
		Possible key lengths (distance dividers)			
Repeated sequence	Distance between repetitions	2	3	5	19
WUU	95			X	x
EEK	200	x		X	
WXIZAYG	190	x		X	x
NUOCZGM	80	x		X	
DOEOY	45		x	X	
GMU	90	x	x	X	

Step 3

- It appears from the table that all periods are divisible by **5**

Vigenère Cryptanalysis : Example Phase 2

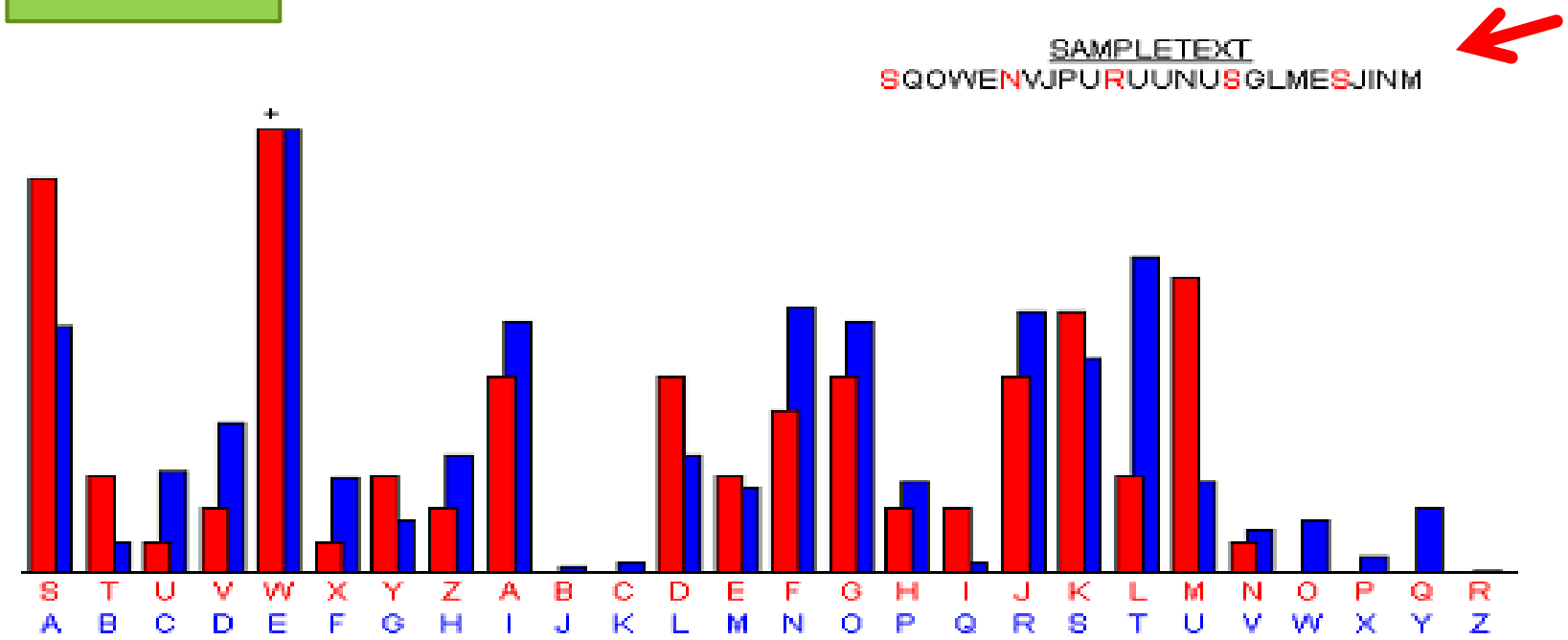
Stage1



- In red, the "modulo 5" frequency analysis
- The blue line represents the frequency diagram of letters in French.

Vigenère Cryptanalysis: Example Phase 2

Stage2



- We shift the diagrams to place the peak of the **W** on the **E.**
- W = 22 and E = 4➔ This is (22 - 4 = 18). It is **S**

Vigenère Cryptanalysis : Example Phases 3, 4, 5, 6

- The key word is: **SCUBA**
- The cryptogram can be decrypted as:

```
SOUVE NTPOU RSAMU SERLE SHOMM ESDEQ UIPAG EPREN NENTD ESALB ATROS VASTE SOISE AUXDE SMERS
QUISU IVENT INDOL ENTSC OMPAG NONSD EVOYA GELEN AVIRE GLISS ANTSU RLESG OUFFR ESAME RSAPE
INELE SONTI LSDEP OSESS URLES PLANC HESQU ECESR OISDE LAZUR MALAD ROITS ETHON TEUXL AISSE
NTPIT EUSEM ENTLE URSGR ANDES AILES BLANC HESCO MMEDE SAVIR ONSTR AINER ACOTE DEUXC EVOYA
GEURA ILECO MMEIL ESTGA UCHEE TVEUL ELUIN AGUER ESIBE AUQUI LESTC OMIQU EETLA IDLUN AGACE
SONBE CAVEC UNBRU LEGUE ULELA UTREM IMEEN BOITA NTLIN FIRME QUIVO LAITL EPOET EESTS EMBLA
BLEAU PRINC EDESN UEESQ UIHAN TELAT EMPET EETSE RITDE LARCH ERBAU DELAI RE
```

Souvent pour s'amuser les hommes d'équipage prennent des albatros, vastes oiseaux des mers, qui suivent, indolents compagnons de voyage, le navire glissant sur les gouffres amers.

A peine les ont-ils déposés sur les planches que ces rois de l'azur, maladroits et honteux, laissent piteusement leurs grandes ailes blanches, comme des avirons, traîner à côté d'eux.

Ce voyageur ailé, comme il est gauche et veule, lui naguère si beau, qu'il est comique et laid. L'un agace son bec avec un brûle-gueule, l'autre mime en boitant l'infirme qui volait.

Le poète est semblable au prince des nuées, qui hante la tempête et se rit de l'archer.

Charles Baudelaire

Affine Cipher

- It is a monoalphabetic cipher.
- The idea is to use an affine function as encryption function of the type **y =(ax+ b) mod26**,
  - a and b are constants,
  - x and y are numbers corresponding to the letters of the alphabet.

Affine cipher

- K = (a,b)
- $E_k(x)$ =ax+ b mod 26
- $D_k(y)$ = $a^{-1}(y-b)$ mod 26
- a^{-1} is the inverse multiplicative function of modulo 26,

i.e.,$aa^{-1} \equiv 1 (mod 26)$

Affine cipher

- For the encryption to be valid (unique), the encryption function must have a single solution (injective).
  - The function $E_k(x)$ has a single solution (for any value of b) if :

$$GCD(a,26)=1$$

Affine cipher: cryptanalysis

- The number of possible keys is 26 times the number of prime elements with 26.
- There are 12 values that are coprime to 26:

  1 3 5 7 9 11 15 17 19 21 23 and 25.

- The number of possible keys is 26*12 = 312.

Affine Cipher – Example 1

K = (17.3), a=17 and b=3

Check: GCD(17,26) =1

➔**valid encryption**

17^{-1} mod 26 = 23 [17*23 = 391 = 1 mod 26]

➔ **a. $a^{-1} \equiv 1 \pmod{26}$ is verified**

- $E_k(x) = 17x + 3 \bmod 26$
- $D_k(y) = 17^{-1}. (y-3) \bmod 26 = 23 * (y-3) \bmod 26$

$= 23\ y - 17 \bmod 26$

Affine Cipher – Example 2

- Let K = (17,3)
- Encrypt the text: CODE

Plain text	C	O	D	E
Ind. Plaintext	2	14	3	4
Ind. Ciphertext	11	7	2	19
Ciphertext	**L**	**H**	**C**	**T**

- Example:
  - E_k (2) = 17* 2 +3% 26 = 37 mod 26 = 11
  - D_k (11) = 23* 11 -17 mod 26 = 2

Affine encryption: cryptanalysis

- we suppose that the ciphertext of r_1 is s_1 and that the ciphertext of r_2 is s_2,
- By solving the system composed by:
  - $r_1a + b = s_1$
  - $r_2a + b = s_2$
- we find a single solution for a and b in Z_{26}.
- If the gcd(a,26)≠ 1, we know that the correspondence is invalid,
- and we try another match (still based on the letter frequency table).

Affine Cryptanalysis: Example

- Encrypted text:
- GHUYI DEGRS YTGOHKEIA AOTDGSBINRGSGHHGNYI ASIR RYOVGEOHGANTGKGR HENNI

Affine Cryptanalysis: Example

- Frequency of letters: G = 10 H = 6
- Assumption :E and T are the most frequent letters in English
- Corresponding equations:

$$\begin{cases} E \rightarrow G: \ E_k(E) = G \\ T \rightarrow H: \ E_k(T) = H \end{cases}$$

$$\begin{cases} 4 \rightarrow 6: \ E_k(4) = 6 \\ 19 \rightarrow 7: \ E_k(19) = 7 \end{cases}$$

Affine Cryptanalysis: Example (3)

- Solve the equations for a and b unknowns:

$$\begin{cases} E_k(4) = 6 \\ E_k(19) = 7 \end{cases}$$

$$\begin{cases} 4a + b = 6 \pmod{26} \\ 19a + b = 7 \pmod{26} \end{cases}$$

$15\ a = 1 \bmod 26$

Therfore: **$a = 7 \pmod{26}$**

Transposition cipher

- A rectangular transposition consists of:
  - Write the message in a rectangular grid.
  - arrange the columns of this grid according to a password given (the position of the letters in the alphabet determines the arrangement of the columns).

Transposition cipher

- Example:
  - Plaintext: SALAM MY STUDENT.
  - The key: SALUT

S	A	L	U	T
3	1	2	5	4
S	A	L	A	M
M	Y	S	T	U
D	E	N	T	X

A	L	S	T	U
1	2	3	4	5
A	L	S	M	A
Y	S	M	U	T
E	N	D	X	T

- Ciphertext: ALSMAYSMUTENDXT

Other encryption techniques

- Vernam
- Playfair,
- ADFGVX
- The machineEnigma
- . . .

Quiz

- The "Coincidence Index Attack" technique used to break:
  - Shift cipher.
  - Vigenère cipher
  - rectangular transposition encryption
  - Affine cipher
- The number of possible keys for Affine cipher is:
  - 26
  - 144
  - 312
  - 676

Questions ?

Moodle:

https://elearning.univ-msila.dz/moodle/course/view.php?id=698