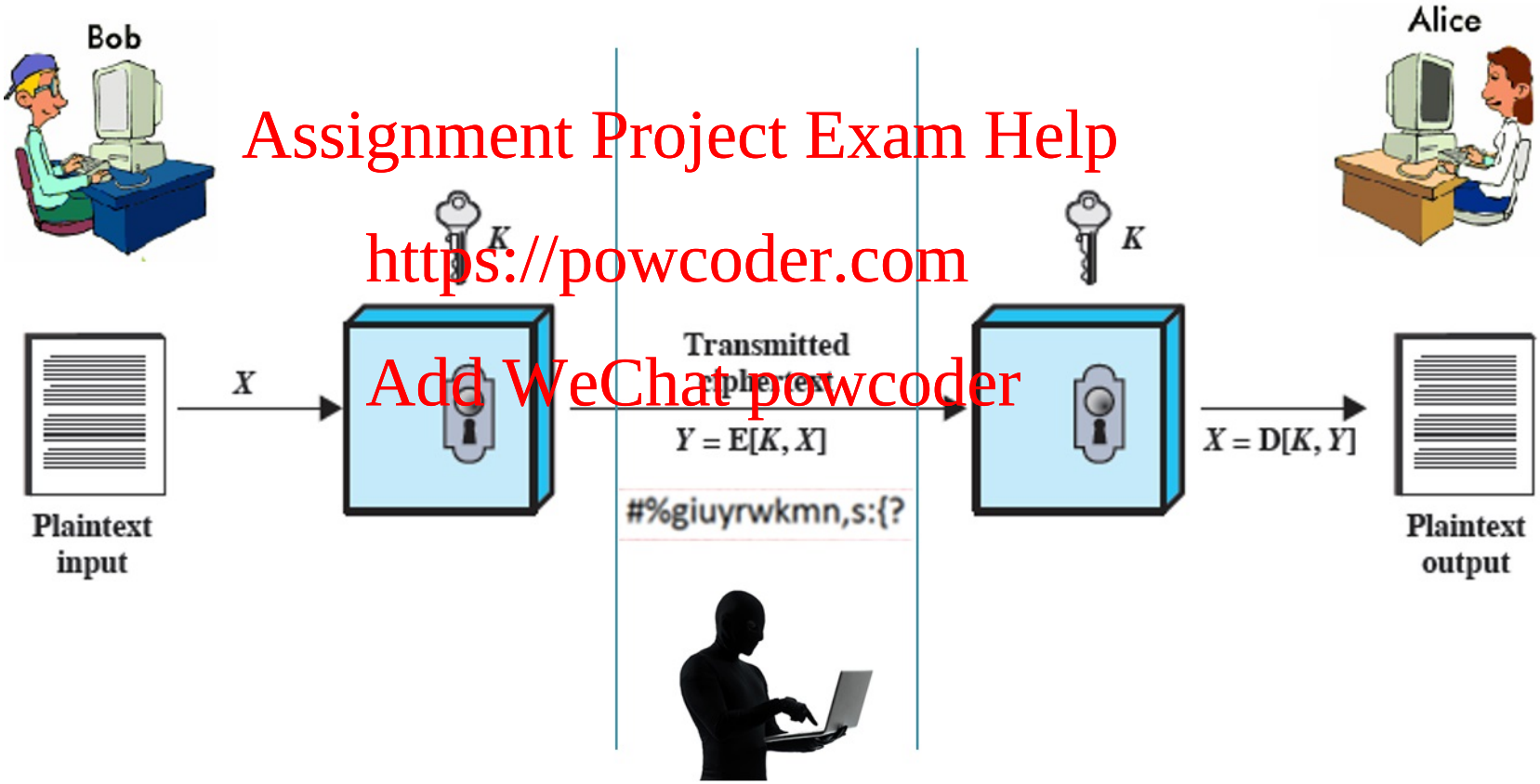


Introduction (cont.)

- **Examples of Cryptanalysis Techniques**

Ciphertext-only attack: The key or plaintext is revealed exclusively by means of the ciphertext. This method is the most difficult. If too little is known of the rules of the ciphertext to be able to exploit them, only one obvious thing remains: trying every possible key. This is called **brute-force attack** (exploiting the key space, exhaustion method). Often, however, it is sufficient to try just a few keys; but more about this later.

Known-plaintext attack: Part of the plaintext is known in addition to the ciphertext, and used to reveal the remaining plaintext, normally by means of the key. This is perhaps the most important cryptanalytic method, because it is much more powerful than a ciphertext-only attack and normally possible: the attacker guesses certain words in the text; the beginning of the text is fixed; known, uncritical plaintexts are encoded with the same key as confidential plaintexts, etc.

passive attacks

hacker does **NOT** have access to crypto-system

Chosen-plaintext attack: In this attack, the adversary has the ability to obtain the encryption of any plaintext(s) of its choice. It then attempts to determine the plaintext that was encrypted to give some other ciphertext.

Chosen-ciphertext attack: The final type of attack is one where the adversary is even given the capability to obtain the decryption of any ciphertext(s) of its choice. The adversary's aim, once again, is then to determine the plaintext that was encrypted to give some other ciphertext (whose decryption the adversary is unable to obtain directly).

active attacks

hacker has access to crypto-system

https://www.u-cursos.cl/usuario/777719ab2ddbbdb16d99df29431d3036/mi_blog/r/1_book-introduction_to_modern_cryptography.pdf

Introduction (cont.)

Ciphertext Only Attacks

(nothing about plaintext is known!)

Known Plaintext Attacks

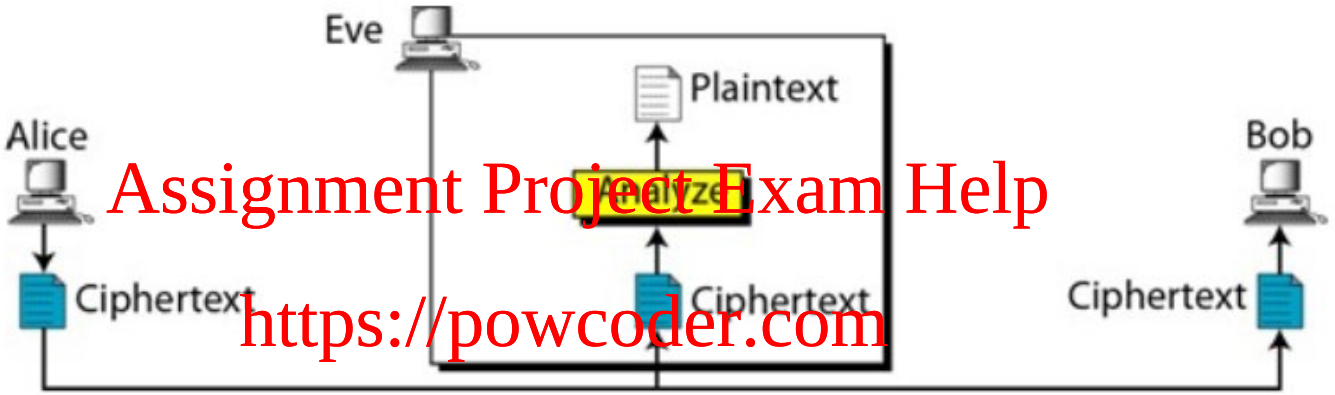
(part of plaintext is known!)

Hello Alice,

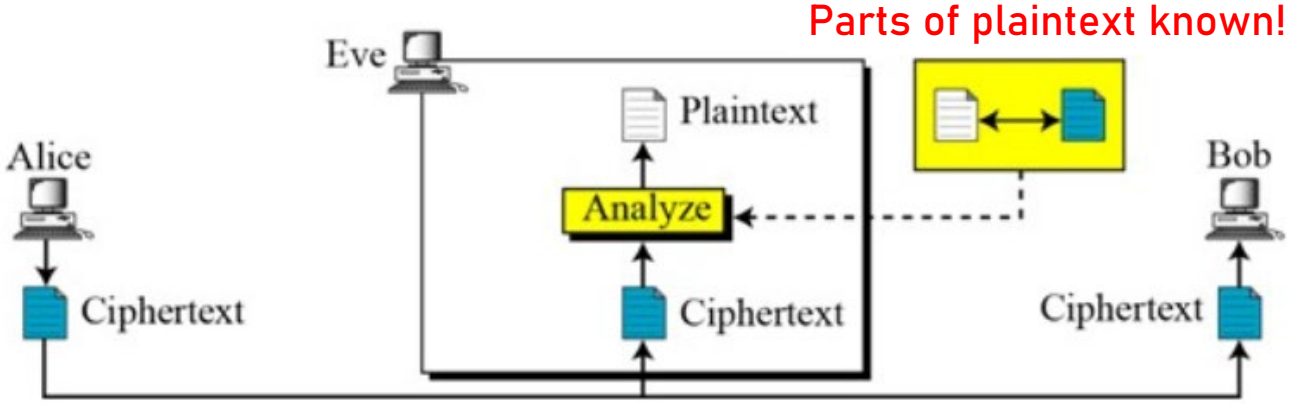
Type of Attack	Known to Cryptanalyst
Ciphertext Only = brute force	• Encryption algorithm ← known • Ciphertext ← obtained
Known Plaintext [accelerated cryptanalysis possible]	• Encryption algorithm • Ciphertext • One or more plaintext-ciphertext pairs formed with the secret key ← can be guessed
Chosen Plaintext [attacker has access to the system with secret key setup (as black box) & can enter chosen plaintexts]	• Encryption algorithm • Ciphertext • Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key
Chosen Ciphertext [attacker has access to the system with secret key setup (as black box) & can enter chosen ciphertexts]	• Encryption algorithm • Ciphertext • Ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key
Chosen Text [attacker has access to the system with secret key setup (as black box) & can enter both, chosen plaintexts and ciphertexts]	• Encryption algorithm • Ciphertext • Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key • Ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key

Introduction (cont.)

Ciphertext Only Attacks: goal is to find the plaintext



Known Plaintext Attacks: goal is to find the key

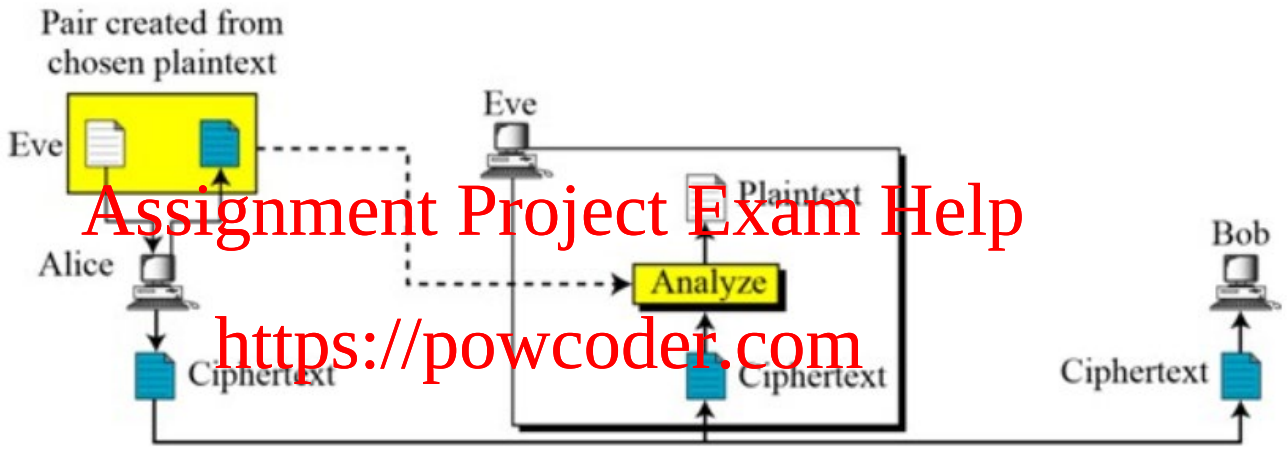


Introduction (cont.)

lunchtime attacks ☺

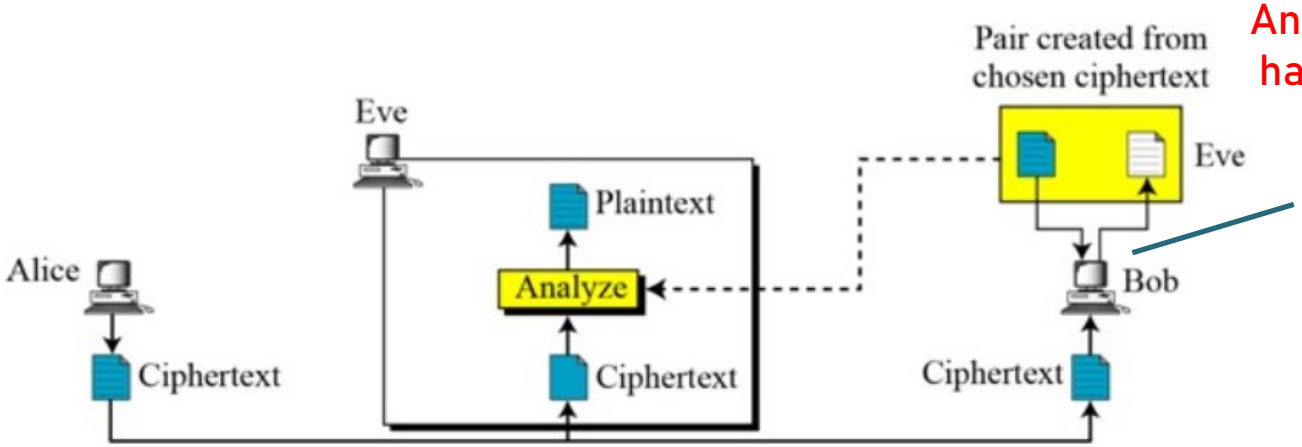
Chosen Plaintext Attacks: goal is to find the key

Any plaintext of hacker's choice!



Chosen Ciphertext Attacks: goal is to find the key

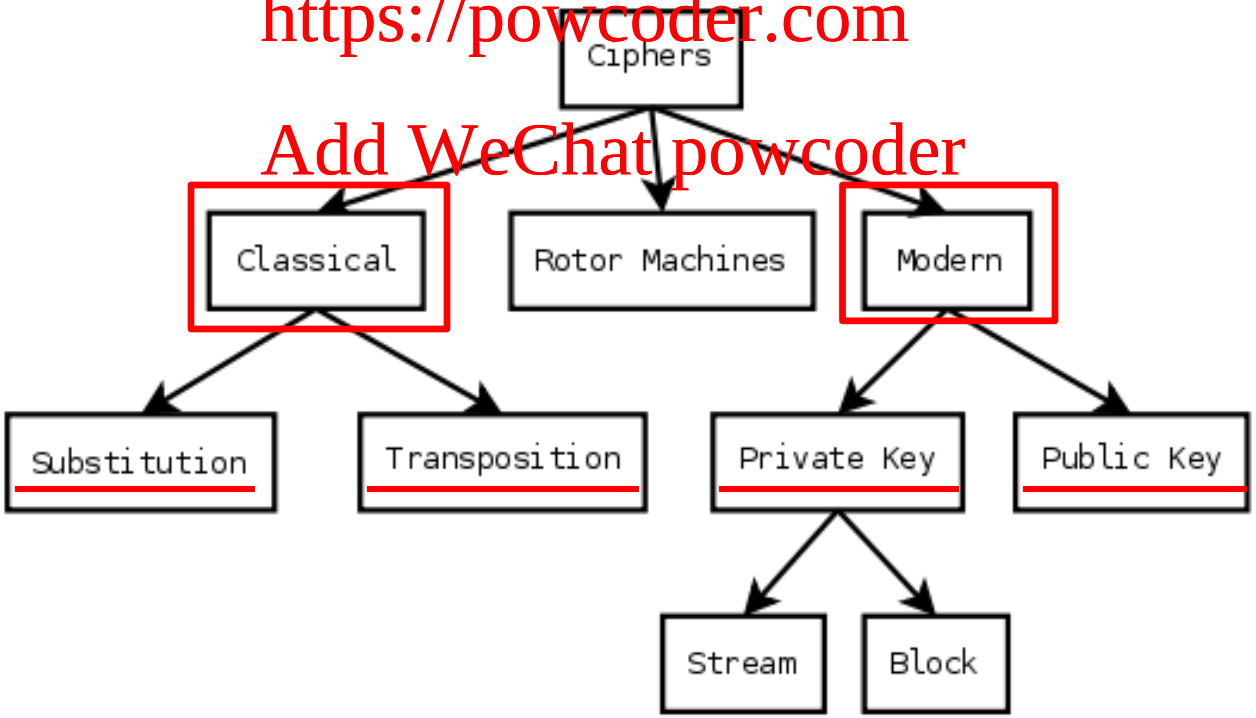
Any ciphertext of hacker's choice!



Eve gets access to the system once, manages to 'crack' the key and then (re)uses this key to decrypt any subsequent messages …

Ciphers

- **History of Cryptography**
  - humans have been using cryptographic techniques for 1000s of years – what have changed are the complexity and creativity of cryptographic techniques



Ciphers (cont.)

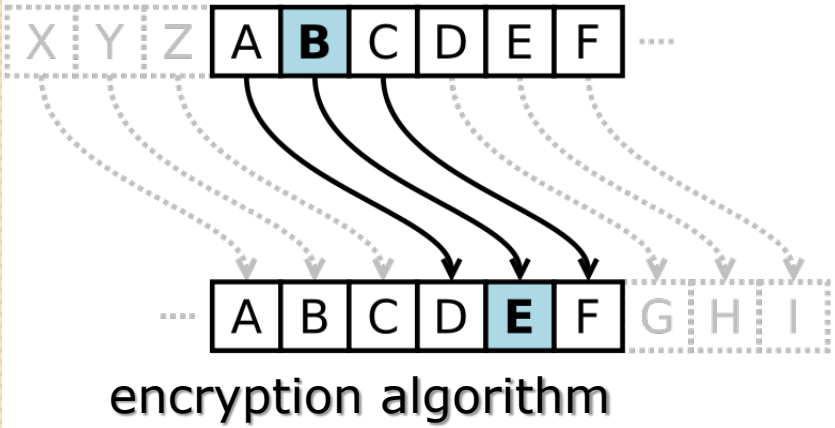
- **Classical vs. Modern Cryptography**
  - **Classical cryptography** - more of an art than science
    - schemes were designed in an ad-hoc manner and then evaluated based on their perceived complexity/cleverness
    - true 'strength' of these schemes was in 'secrecy' of their respective protocols
  - **Modern cryptography** - based on scientific foundations
    - the strength is NOT in secrecy of protocols but in sound mathematical and computational principles
    - it is now possible to formally argue about the security protocols
    - used for more than just data confidentiality - can protect data integrity, enable user authentication, etc.

Classical Ciphers

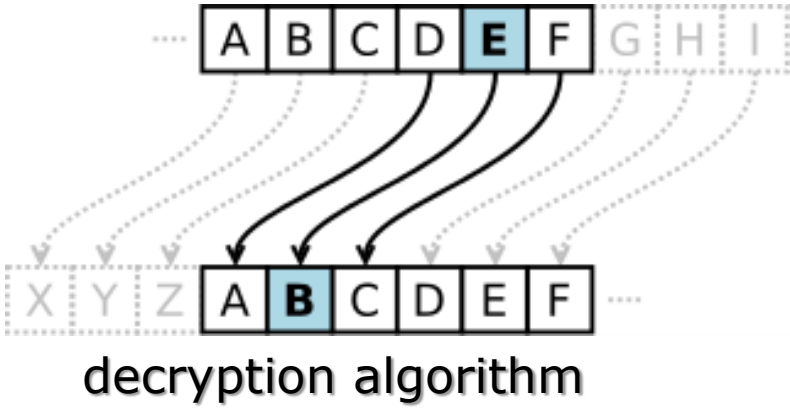
- **Substitution Cipher** – the units of plaintext (letters) are kept in the same original sequence, but the units themselves are altered

- **Caesar Cipher** – substitution cipher in which each letter in the plaintext is replaced by a letter some fixed number of positions down the alphabet

Example: Caesar Cipher with k=3



encryption algorithm



decryption algorithm

Classical Ciphers (cont.)

Example: Caesar cipher encryption with k=3

Ciphertext: WKH TXLFN EURZQ IRA MXPSV RYHU WKH ODCB GRJ

Plaintext: THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG

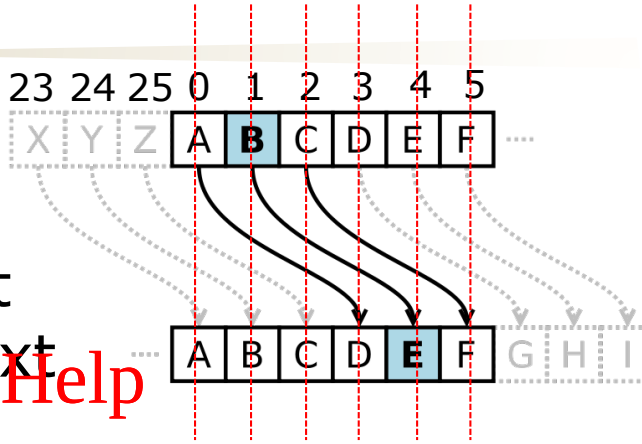
https://www.cs.uri.edu/cryptography/classicalshiftdemo.htm

http://www.simonsingh.net/The_Black_Chamber/caesar.html

Caesar cipher is easy to break.
Keyspace = 25 different keys

Classical Ciphers (cont.)

Represent letters with numbers!



- **Cesar Cipher as an Algorithm**

T_i - *i*-th character of the plain text
C_i - *i*-th character of the cipher text
i = 0, 1, 2, .. , m-1
m - length of the alphabet
k - shift

Encryption: $\mathbf{C_i = (T_i + k) \bmod m}$

Decryption: $\mathbf{T_i = (C_i - k) \bmod m}$

NOTE:

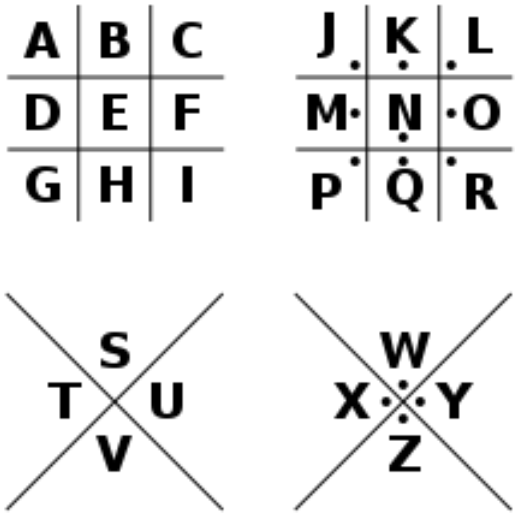
-b mod m = (-b + m) mod m

http://en.algoritmy.net/article/40203/Caesar-cipher

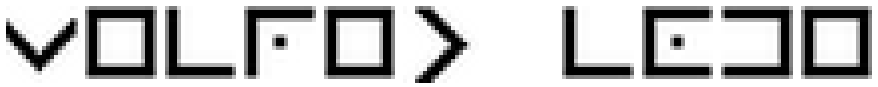
Classical Ciphers (cont.)

aka masonic or tic-tac-toe cipher

- **Pigpen Cipher** – substitution cipher in which each letter is replaced with a **graphical symbol**
  - alphabet is written in 4 grids shown below
  - each letter is replaced with a symbol that corresponds to the portion of the pigpen grid that contains the letter
  - used by Freemasons in the 18th century to keep their records private



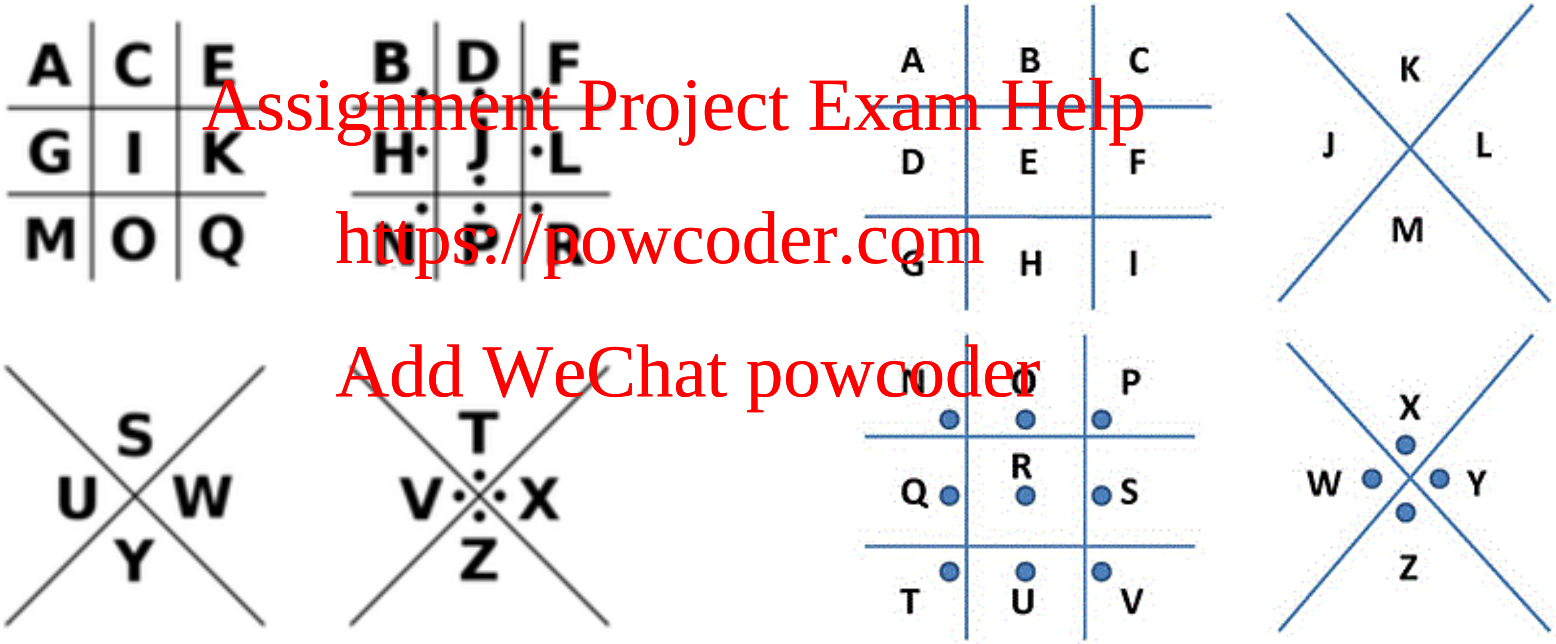
Example: Pigpen cipher



SECRET CODE

Classical Ciphers (cont.)

Example: Pigpen Cipher variants

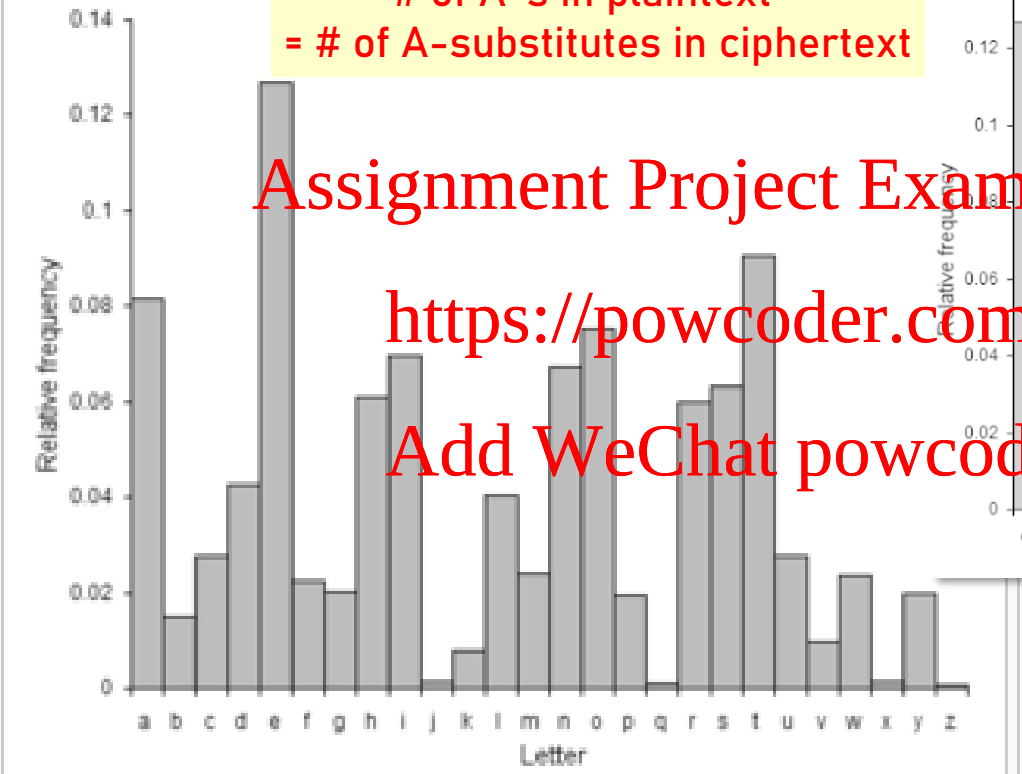


https://crypto.interactive-maths.com/pigpen-cipher.html

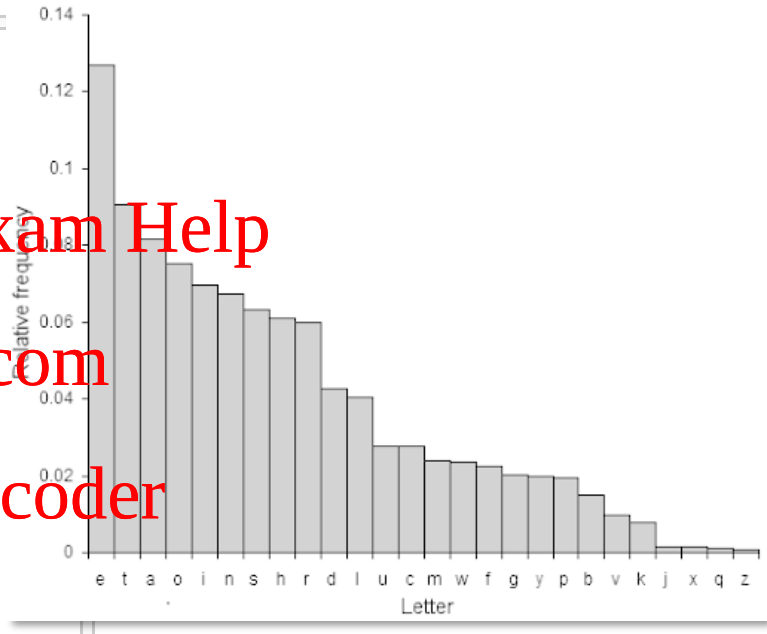
Classical Ciphers (cont.)

Example: How to break a simple substitution cipher?

# of A-s in plaintext =
= # of A-substitutes in ciphertext

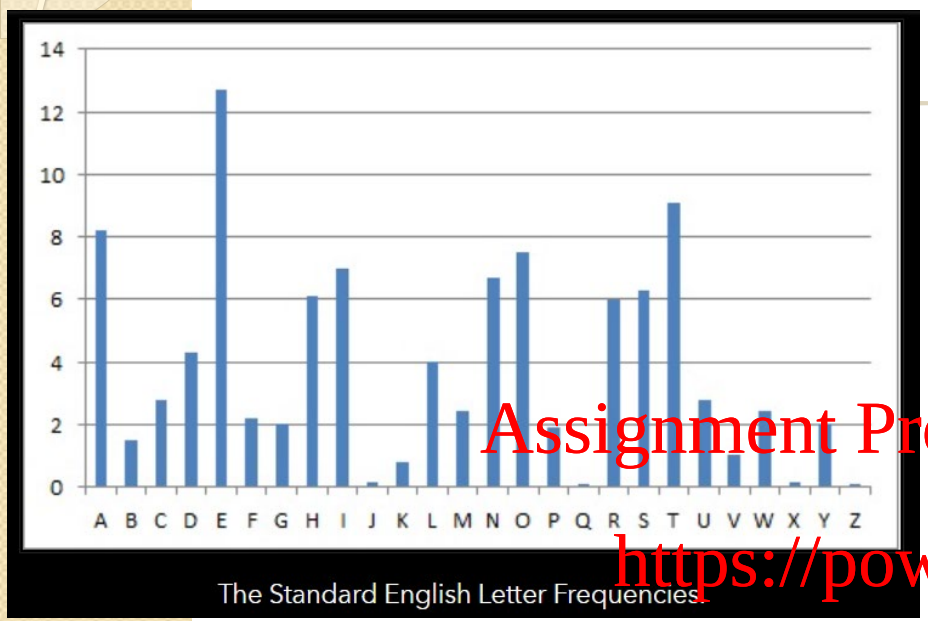


The distribution of letters in a typical sample of English language text has a distinctive and predictable shape. A Caesar shift "rotates" this distribution, and it is possible to determine the shift by examining the resultant frequency graph.

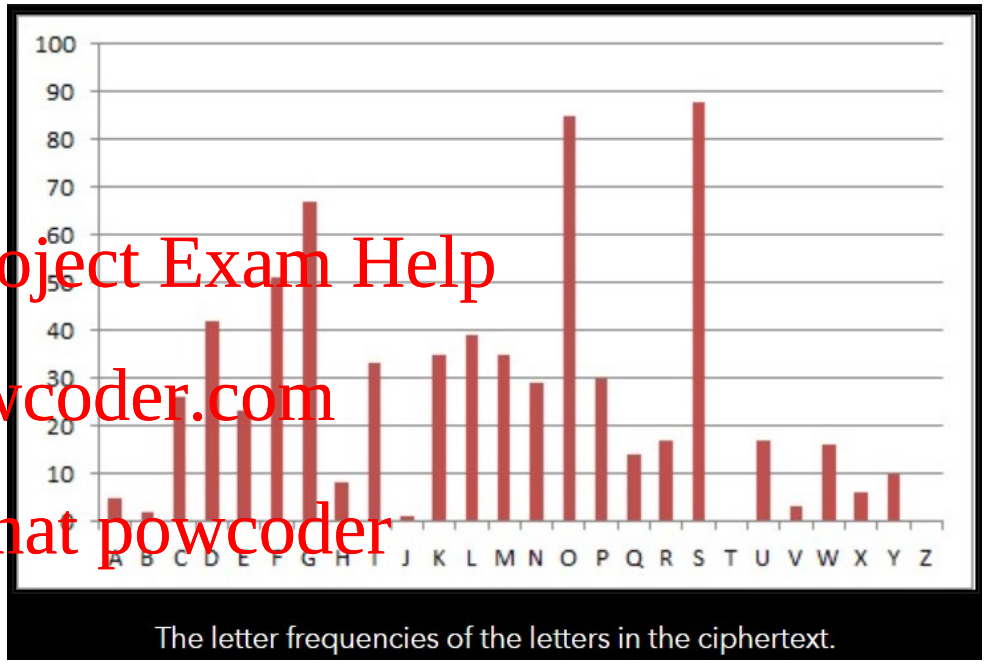


http://www.usafa.edu/df/dfe/dfer/centers/accr/tools/ShiftCipherApplet.html

Example: breaking a cipher using FREQUENCY analysis



The Standard English Letter Frequencies.



The letter frequencies of the letters in the ciphertext.

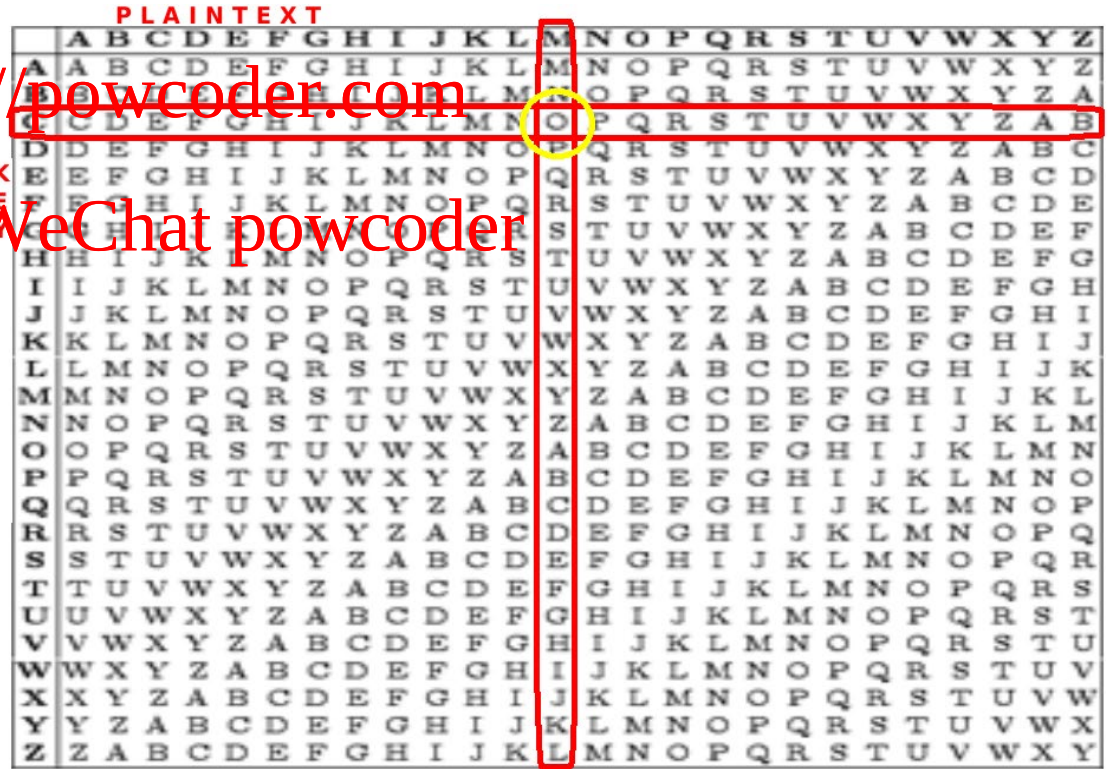
"Now that we have all the frequencies of ciphertext letters, we can start to make some substitutions. We see that the most common ciphertext letter is "S", closely followed by "O". From the chart and table above, we can guess that these two letters represent "e" and "t" respectively, and after making these substitutions we get … "

https://crypto.interactive-maths.com/frequency-analysis-breaking-the-code.html

Classical Ciphers (cont.)

- **Polyalphabetic / Vigenere Cipher** – **complex** substitution cipher - instead of shifting each character by the same number, characters located at different positions are shifted by different numbers = key keeps changing!

- key (word) must be provided
- key is aligned with plaintext – key-letter determines the value of cipher-letter



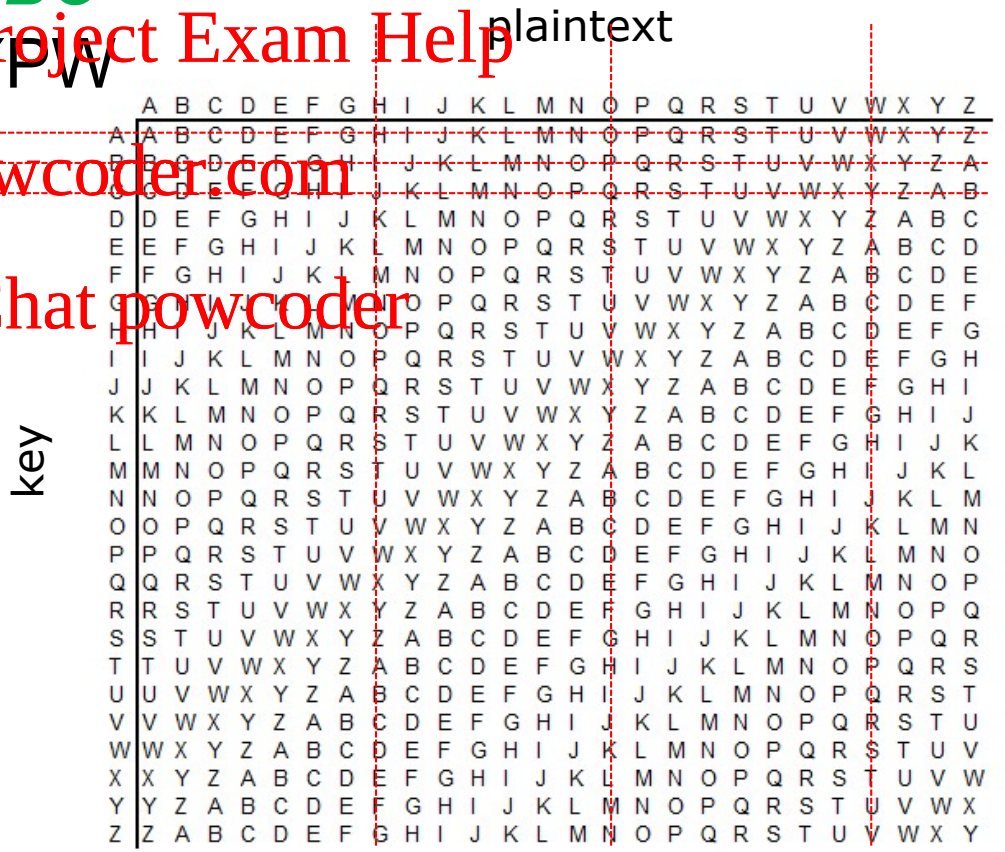
Classical Ciphers (cont.)

Example: Viegenere Cipher - decryption using the table

Plaintext: HOW ARE YOU

Key: *ABC ABC ABC*

Ciphertext: HPY ASG YPW



http://www.simonsingh.net/The_Black_Chamber/vigenere_square_tool.html

Classical Ciphers (cont.)

- **Vigenere Cipher as an Algorithm**

T_i - *i*-th character of the plain text
C_i - *i*-th character of the cipher text
K_i - *i*-th character of the key phrase
i = 0, 1, 2, ..., m-1
m - length of the alphabet

Encryption: $\mathbf{C_i = (T_i + K_i) \bmod m}$

Decryption: $\mathbf{T_i = (C_i - K_i) \bmod m}$

http://en.algoritmy.net/article/45623/Vigenere-cipher

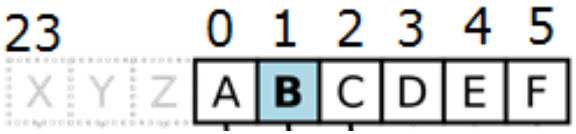
Classical Ciphers (cont.)

Example: Viegenere Cipher - encryption using algorithm

Open text: ATTACK AT DAWN

Key phrase: CAT

Length of the alphabet: 26



A	+	C	=	0	+	2	=	C
T	+	A	=	19	+	0	=	T
T	+	T	=	19	+	19	=	M
A	+	C	=	0	+	2	=	C
C	+	A	=	2	+	0	=	C
K	+	T	=	10	+	19	=	D
A	+	C	=	0	+	2	=	C
T	+	A	=	19	+	0	=	T
D	+	T	=	3	+	19	=	W
A	+	C	=	0	+	2	=	C
W	+	A	=	22	+	0	=	W
N	+	T	=	13	+	19	=	G