Symmetric Cipher Model

Altayeva Aigerim

aigerim.muit@gmail.com

Introduction

Symmetric encryption, also referred to as ***conventional encryption*** or ***single-key encryption***, was the only type of encryption in use prior to the development of ***public-key encryption*** in the 1970s. It remains by far the most widely used of the two types of encryption.

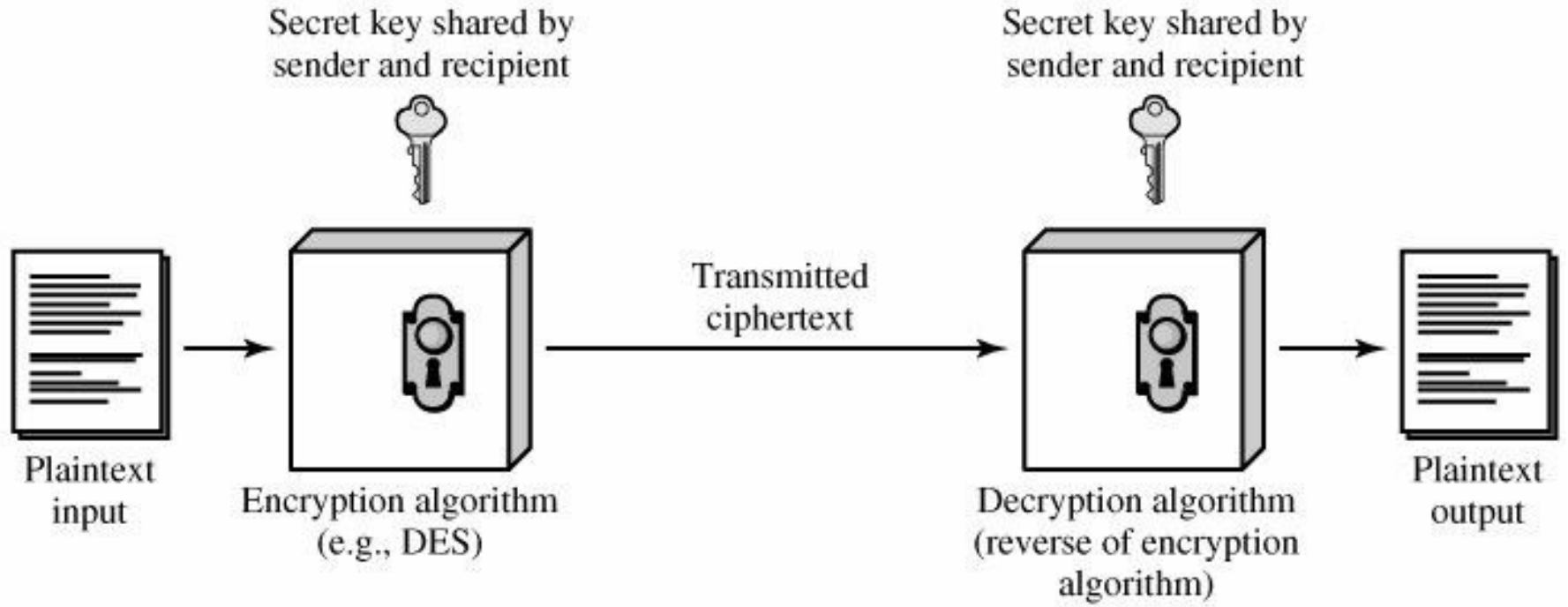
Beginning with a look at a general model for the symmetric encryption process; this will enable us to understand the context within which the algorithms are used

Content

1. Symmetric cipher
   - Secure Use of Conventional Encryption
   - Symmetric Encryption Scheme
2. Cryptographic systems
3. Cryptanalysis
   - Cryptanalytic Attacks
   - Brute-force attack
     - Brute-Force Cryptanalysis of Caesar Cipher
4. Monoalphabetic Ciphers
   - Breaking Monoalphabetic Cipher

Symmetric cipher

- A form of cryptosystem in which encryption and decryption are performed using the same key. Also known as ***conventional encryption***.
- A symmetric encryption scheme has five ingredients.



Secure Use of Conventional Encryption

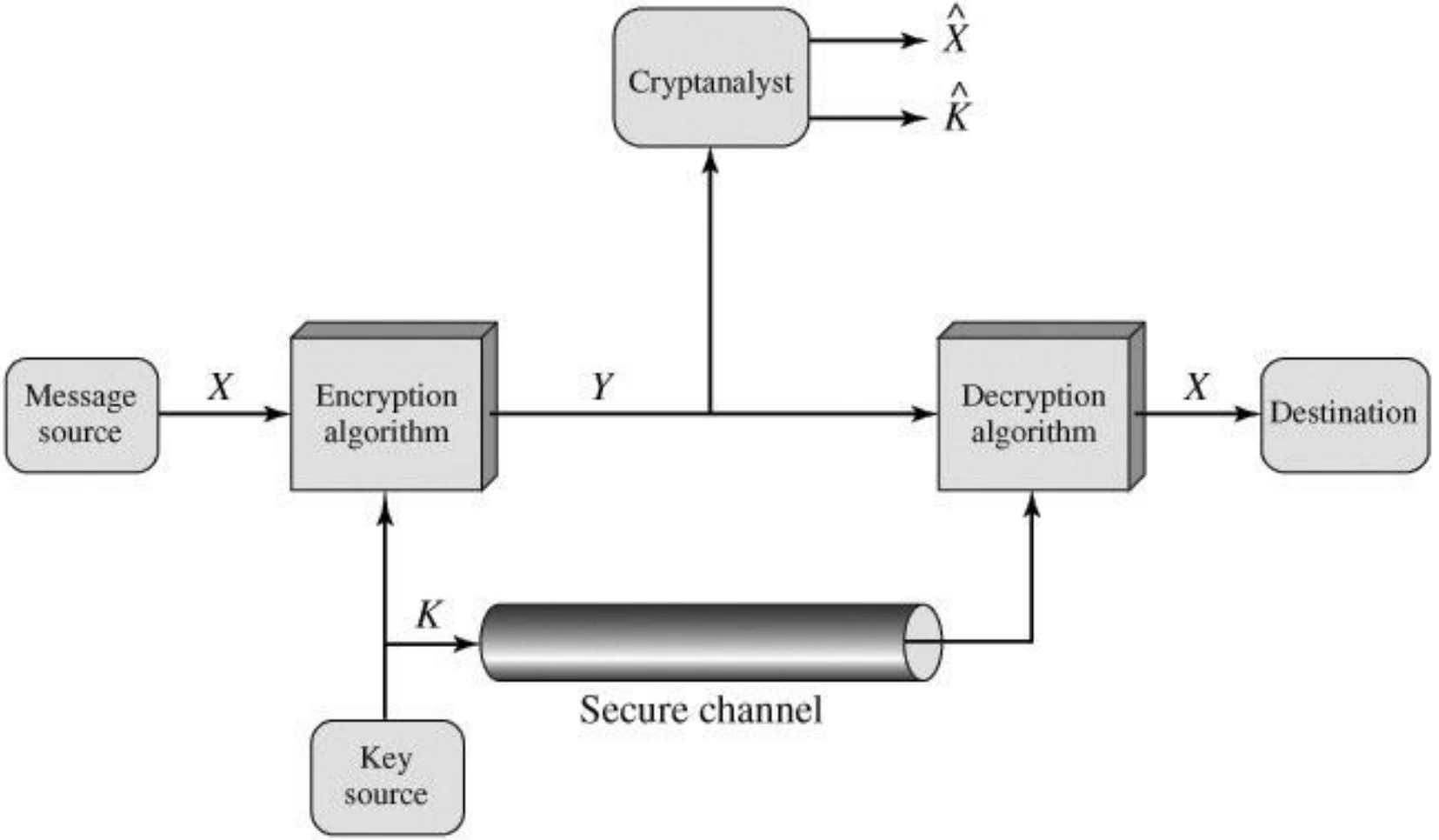
Two requirements for secure use of conventional encryption:

1. ***Strong algorithm*** – an opponent unable to decipher the ciphertext or figure out the key.

2. Shared secret key – sender and receiver must have obtained copies of the secret key in a secure fashion and must keep the key secure.

Symmetric Encryption Scheme

- We do not need to keep the algorithm secret; we need to keep only the key secret.



Cryptographic systems

Characterized along three independent dimensions:

1. The type of operations used for transforming plaintext to ciphertext. All encryption algorithms are based on two general principles:

- ***Substitution:*** the plaintext is mapped into another element
- ***Transposition:*** the plaintext elements are rearranged

2. The number of keys used.

- ***Symmetric:*** both sender and receiver use the same key (a.k.a. single-key, secret-key, or conventional encryption)
- ***Asymmetric:*** the sender and receiver use different key (a.k.a. two-key, or public-key encryption)

3. The way in which the plaintext is processed.

- ***A block-cipher:*** processes the input one block of elements at a time, producing an output block for each input block.
- ***A stream-cipher:*** processes the input elements continuously, producing output one element at a time, as it goes along

Cryptanalysis

Two general approaches to attacking a conventional encryption scheme:

- ***Cryptanalysis:*** exploits the characteristics of the algorithm to attempt to deduce a specific plaintext or to deduce the key being used.
- ***Brute-force attack:*** tries every possible key on a piece of ciphertext until an intelligible translation into plaintext is obtained

Cryptanalytic Attacks

- ***Ciphertext only:***
  - Encryption algorithm
  - Ciphertext
- ***Known plaintext:***
  - Encryption algorithm
  - Ciphertext
  - One or more plaintext-ciphertext pairs formed with the secret key

- ***Chosen plaintext:***
  - Encryption algorithm
  - Ciphertext
  - Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key
- ***Chosen ciphertext:***
  - Encryption algorithm
  - Ciphertext
  - Purported ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key

- ***Chosen text:***
  - Encryption algorithm
  - Ciphertext
  - Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key
  - Purported ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key

A Brute-Force Attack

- Trying **every possible key** until an intelligible translation of the ciphertext into plaintext is obtained.
- On average, half of all possible keys must be tried to achieve success.

Brute-Force Cryptanalysis of Caesar Cipher

Three important characteristics of this problem enabled us to use a brute-force cryptanalysis:

1. The encryption and decryption algorithms are known.

2. There are only 25 keys to try.

3. The language of the plaintext is known and easily recognizable.

Example: Let's encipher some text using Caesar cipher with the secret key is *3*.

plain: meet me after the toga party

cipher: PHHW PH DIWHU WKH WRJD SDUWB

Simply try all the 25 possible keys. Below shown the results.

KEY						
		PHHW	PH	DIWHU	WKH	WRJD	SDUWB
	1	oggv	og	chvgt	vjg	vqic	rctva
	2	nffu	nf	bgufs	uif	uphb	qbsuz
	3	meet	me	after	the	toga	party
	4	ldds	ld	zesdq	sgd	snfz	ozqsx
	5	kccr	kc	ydrcp	rfc	rmey	nyprw
	6	jbbq	jb	xcqbo	qeb	qldx	mxoqv
	7	iaap	ia	wbpan	pda	pkcw	lwnpu
	8	hzzo	hz	vaozm	ocz	ojbv	kvmot
	9	gyyn	gy	uznyl	nby	niau	julns
	10	fxxm	fx	tymxk	max	mhzt	itkmr

Monoalphabetic Ciphers

- With only 25 possible keys, the Caesar cipher is far from secure. A dramatic increase in the key space can be achieved by allowing an arbitrary substitution.

  plain: 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

  cipher: 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

- If instead, the "cipher" line can be any permutation of the 26 alphabetic characters, then there are 26! or greater than 4×10^{26} possible keys.

Breaking Monoalphabetic Cipher

The ciphertext to be solved is

UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXU

DBMETSXAIZVUEPHZHMDZSHZOWSFPAPPDTSV

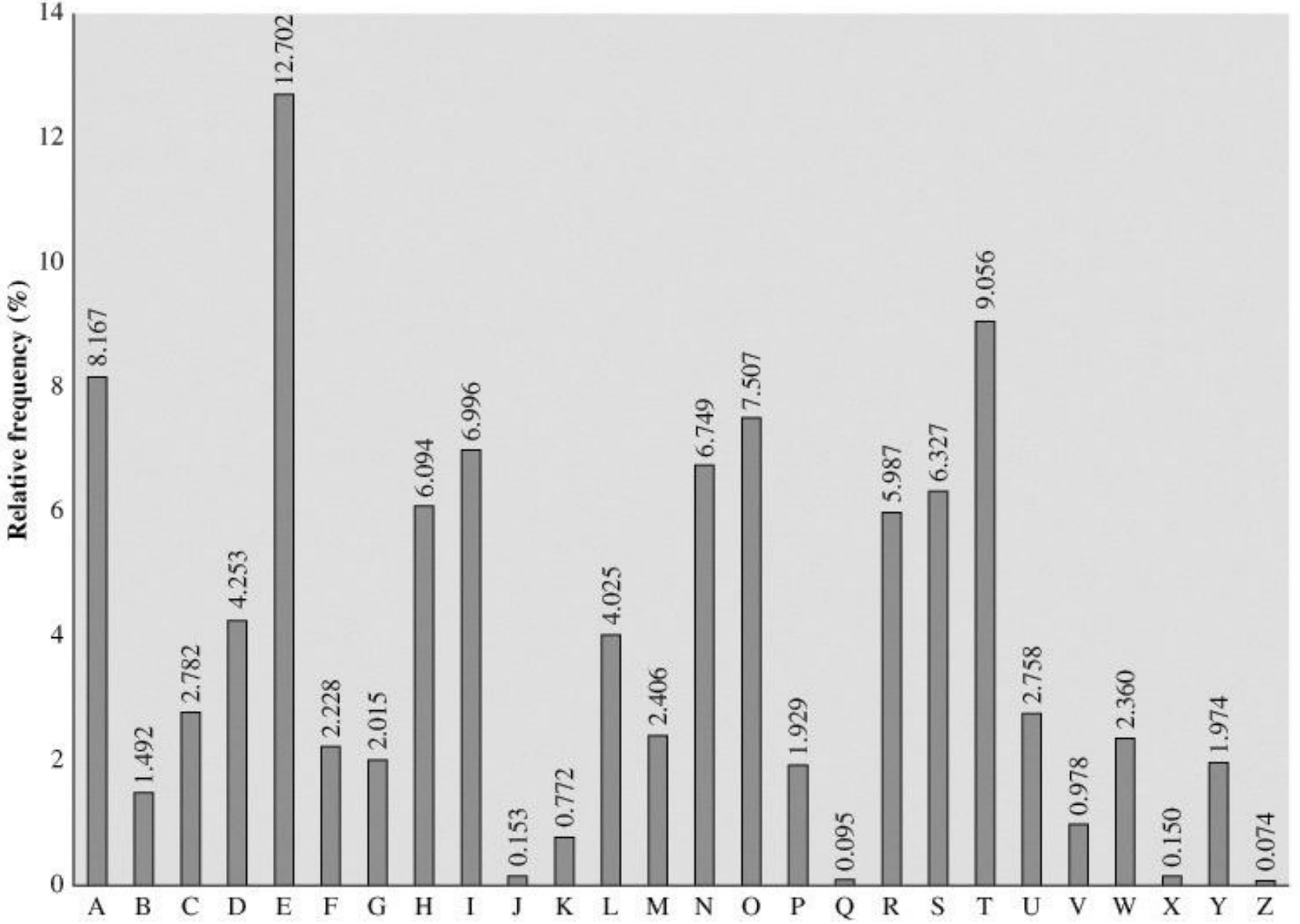
PQUZWYMXUZUHSXEPYEPOPDZSZUFPOMBZWPF

UPZHMDJUDTMOHMQ

The relative frequency of the letters

P 13.33	H 5.83	F 3.33	B 1.67	C 0.00
Z 11.67	D 5.00	W 3.33	G 1.67	K 0.00
S 8.33	E 5.00	Q 2.50	Y 1.67	L 0.00
U 8.33	V 4.17	T 2.50	I 0.83	N 0.00
O 7.50	X 4.17	A 1.67	J 0.83	R 0.00
M 6.67				

Relative Frequency of Letters in English Text



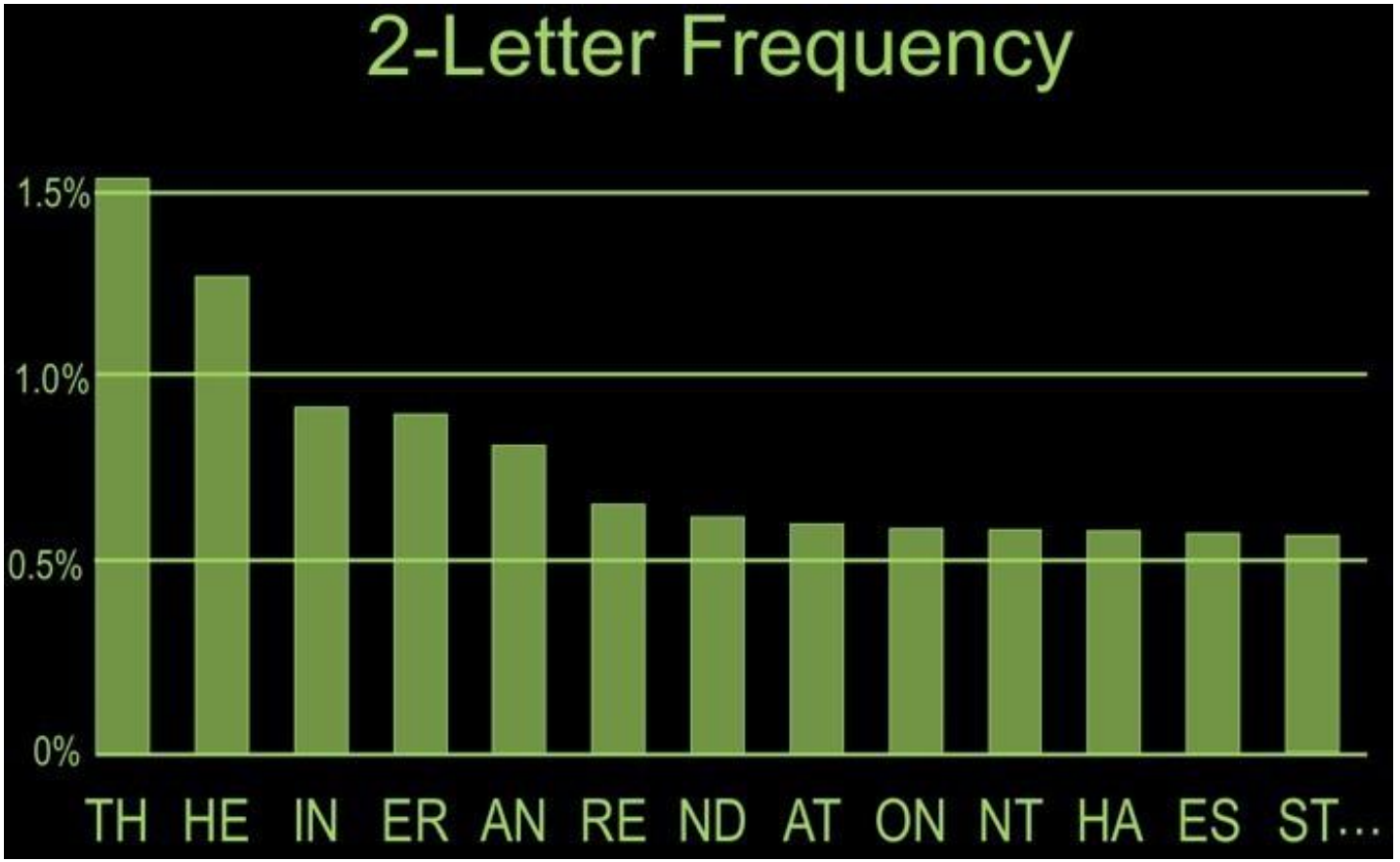
Comparing two previously shown tables that cipher letters ***P*** and ***Z*** are the equivalents of plain letters ***e*** and ***t***, but it is not certain which is which

The letters ***S***, ***U***, ***O***, ***M***, and ***H*** are all of relatively high frequency and probably correspond to plain letters from the set ***{a, h, i, n, o, r, s}***.

The letters with the lowest frequencies (namely, ***A, B, G, Y, I, J***) are likely included in the set ***{b, j, k, q, v, x, z}***.

A more systematic approach is to look for other regularities. For example, certain words may be known to be in the text. Or we could look for repeating sequences of cipher letters and try to deduce their plaintext equivalents.

A powerful tool is to look at the frequency of two-letter combinations, known as digrams.



The most common digram in cipher is ZW, which appears three times. So we make the correspondence:

$$Z \rightarrow \text{ t and } W \rightarrow \text{ h.}$$

So far, then, we have

UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBM

EtTSaXAIZ e e te a that e e a a

VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZU

HSX e t ta t ha e ee a e th t a

EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDT

MOHMQ e e e tat e the t

Only four letters have been identified, but already we have quite a bit of the message.

Continued analysis of frequencies plus trial and error should easily yield a solution from this point.

it was disclosed yesterday that several informal but direct contacts have been made with political representatives of viet cong in moscow

The complete plaintext, with spaces added between words, above.

Refences

- http://www.lunarpages.com/uptime/holding-line-aga
- http://www.mathpickle.com/K-12/Blog/Entries/2010
- Cryptography and Network Security Principles and Practices, Fourth Edition, William Stallings
  - Chapter 2. Classical Encryption Techniques
    - 2.1. Symmetric Cipher Model
    - 2.2. Substitution Techniques