SYMMETRIC ENCRYPTION

Historical ciphers

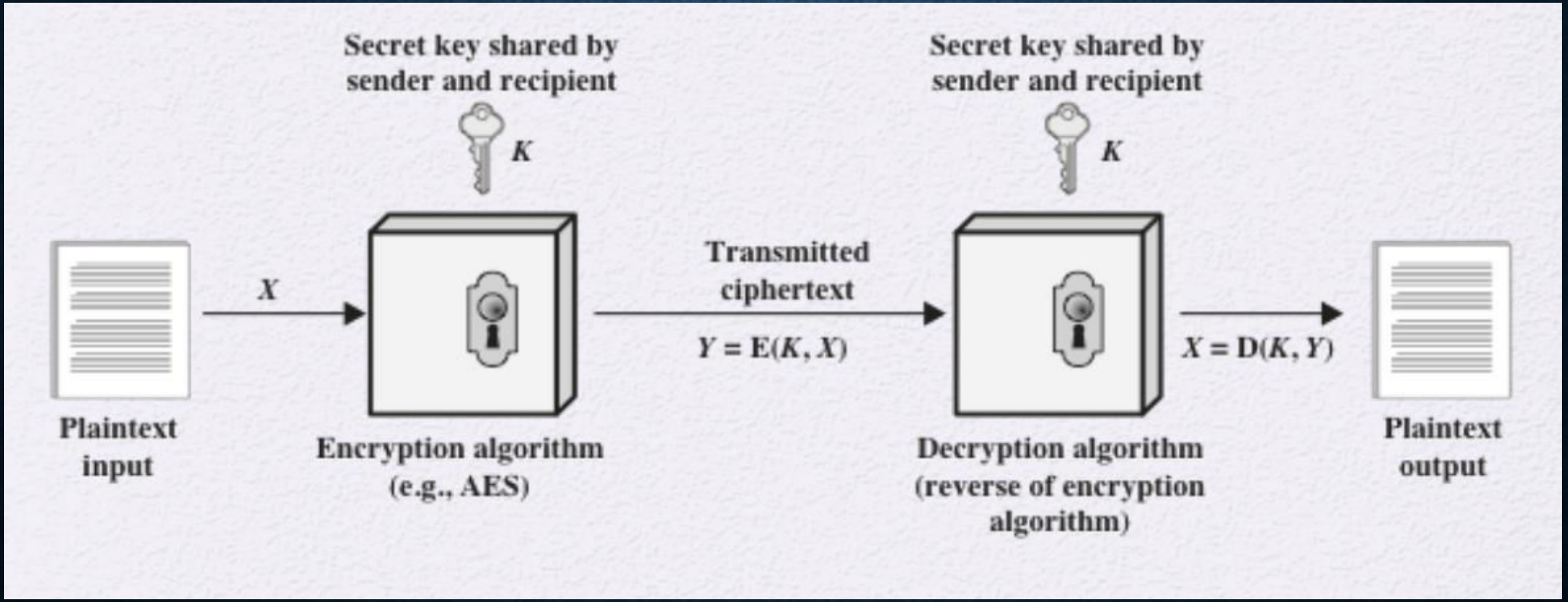
SYMMETRIC ENCRYPTION

- A model of encryption where both the sender and the recipient use the same secret key to encode and decode the message.
- The only type of encryption in use prior to the development of public-key encryption in the 1970s
- Remains by far the most widely used of the two types of encryption
- Has a wide reangeof applications

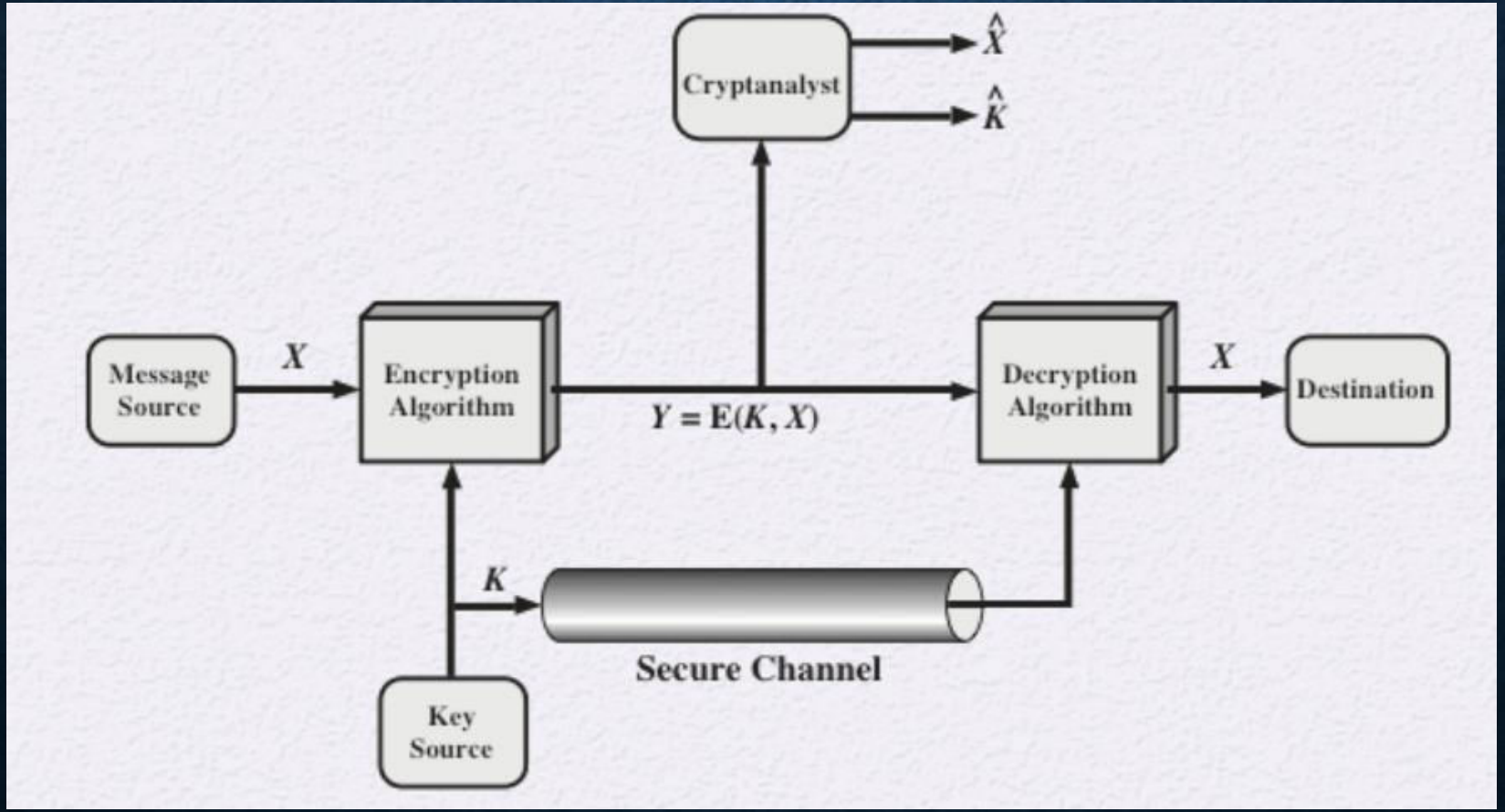
SOME TERMS

- Message
  - The message that has to be communicated between the 2 parties.
- Channel
  - The medium through which the message is transmitted.
- Plaintext
  - The original message
- Ciphertext
  - The encoded message
- Encryption or Enciphering
  - Converting plaintext to ciphertext
- Decryption or Deciphering
  - Restoring the plaintext from the ciphertext

MODEL FOR SYMMEIRC ENCRYPTION



SECURITY MODEL FOR SYMMETRIC ENCRYPTION



SECURITY THROUGH OBSCURITY

- Security through obscurity
  - The philosophy that the secrecy of the design or implementation is the main method of providing security
  - This is not a realistic outlook to maintain while designing the security aspect of any system or application.
  - Too many people will have access to the end product. If we depend on the "algorithm" for security, then it will eventually be disclosed or reverse engineered.
- Kerchoffs' assumption aka Kerchoff's Principle
  - The adversary knows all details of the encryption function except the secret key

CLASSIFYING CRYPTOGRAPHIC PROTOCOLS

Based on the operation used:

- Confusion
  - Uses substitution as the main operation. Replaces one character or set of characters with another.
- Diffusion
  - Uses Transposition to change the order of the characters in the message to render the message unintelligible.
- Most cryptographic protocols use a mixture of both.

CLASSIFYING CRYPTOGRAPHIC PROTOCOLS

- Based on the number of keys used
- Symmetric
  - Uses the same secret key on both ends, for encryption and decryption
- Asymmetric
  - Uses a different key for encryption and decryption, and relies on mathematical principles for both secrecy and retrieval of information.

CLASSIFYING CRYPTOGRAPHIC PROTOCOLS

- Based on the method of processing the plaintext
- Block Ciphers
  - Process the plaintext in "blocks". These ciphers work on the plaintext by splitting them into chunks and then encrypting one chunk at a time.
- Stream ciphers
  - These ciphers process the plaintext as it is produced, results in a stream of enciphered output.

CRYPTANALYSIS AND BRUTE-FORCE ATTACK

- Brute Force Attacks:
  - Attacker tries every possible key on a piece of ciphertext until an intelligible translation into plaintext is obtained
  - On average, half of all possible keys must be tried to achieve success
- Cryptanalysis
  - Uses the nature of the algorithm plus some knowledge of the general characteristics of the plaintext
  - The characteristics of the algorithm are analysed and exploited to find a specific plaintext or the keybeing used

BRUTE FORCE ATTACKS

- Try 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
- To supplement the brute-force approach, some degree of knowledge about the expected plaintext is needed, and some means of automatically distinguishing plaintext from garble

TYPES OF ATTACKS

Type of Attack	Known to Cryptanalyst
Ciphertext Only	Encryption algorithm, ciphertext
Known Plaintext	Encryption algorithm, ciphertext, one or more plaintext-ciphertext pairs with the corresponding secret keys.
Chosen Plaintext	Encryption algorithm, ciphertext, plaintext message chosen by the cryptanalyst along with the corresponding ciphertetx and secret key
Chosen Ciphertext	Encryption algorithm, ciphertext, ciphertext chosen by the cryptanalyst, along with its decrypted plaintext and the secret key

SECURITY OF ENCRYPTION

- Unconditionally secure
  - No matter how much time or computational power an opponent has, it is impossible to decrypt the ciphertext
- Computationally secure
  - The cost of breaking the cipher exceeds the value of the encrypted information
  - The time required to break the cipher exceeds the useful lifetime of the information

SUBSTITUTION TECHNIQUES

- Substitution ciphers are confusion ciphers.
- There are several ways to produce confusion while encrypting, including but not limited to :
    1. The letters of plaintext can be replaced by other letters or numbers or symbols
    2. The plaintext can be viewed as a sequence of bits, and plaintext bit patterns can be replaced with ciphertext bit patterns
- Adding confusion makes the relation between the key and the ciphertext complex

CAESAR CIPHER

- A monoalphabetic circular shift cipher.
- The first known example of encrypted text being “sent in the clear”.
- Used by Julius Caesar for his personal communication.
- Replacing each letter of the alphabet with the letter standing 3 places further down the alphabet.
- Alphabet is wrapped around so that the letter following Z is A.
- `plaintext:  meet  me  after  the  toga  party`
- `ciphertext:  PHHW  PH  DIWHU  WKH  WRJD  SDUWB`
- While Caesar used a 3 letter, shift, it can be applied for any k-letter shift.

CAESAR CIPHER ALGORITHM

- Can define transformation as:

```
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
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
```

- Mathematically give each letter a number

```
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
```

- Algorithm can be expressed as:

$$c = E(3, p) = (p + 3) \bmod (26)$$

- A shift may be of any amount, so that the general Caesar algorithm is:

$$C = E(k, p) = (p + k) \bmod 26$$

- Where k takes on a value in the range 1 to 25; the decryption algorithm is simply:

$$p = D(k, C) = (C - k) \bmod 26$$

CAESAR CIPHER – EASY BRUTE FORCE CRYPTANALYSIS

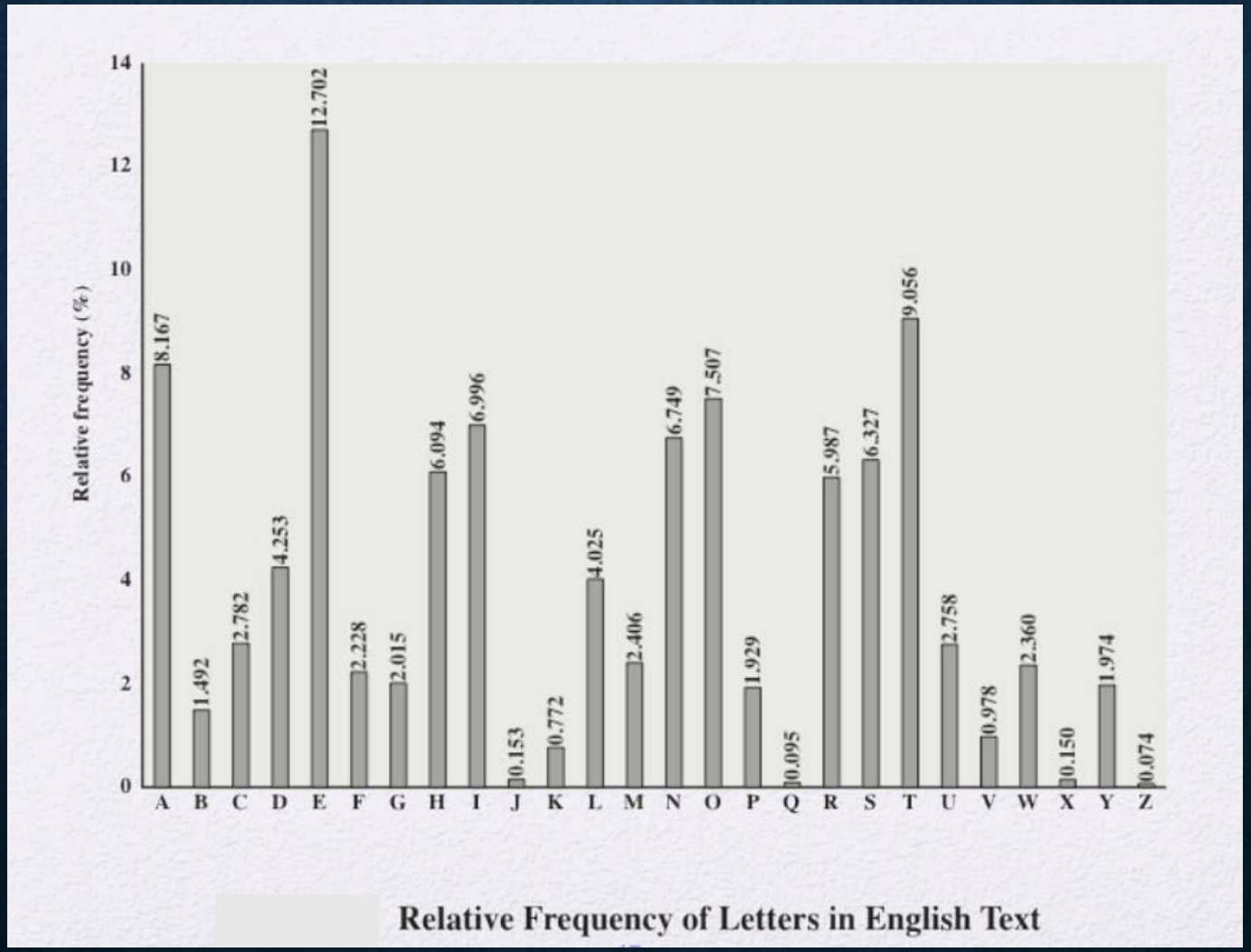
KEY	PHHW PH DIWHU WKH WRJD SDUWB
1	oggv og chvgt vjg vqic rctva
2	nffu nf bgufs uif uphb qbsuz
3	meet me after the toga party
4	ldds ld zesdq sgd snfz ozqsx
5	kccr kc ydrcp rfc rmey nyprw
6	jbbq jb xcqbo qeb qldx mxoqv
7	iaap ia wbpan pda pkcw lwnpu
8	hzzo hz vaozm ocz ojbv kvmot
9	gyyn gy uznyl nby niau julns
10	fxxm fx tymxk max mhzt itkmr
11	ewwl ew sxlwj lzw lgys hsjlq
12	dvvk dv rwkvi kyv kfxr grikp
13	cuuj cu qvjuh jxu jewq fqhjo
14	btti bt puitg iwt idvp epgin
15	assh as othsf hvs hcuo dofhm
16	zrrg zr nsgre gur gbtn cnegl
17	yqqf yq mrfqd ftq fasm bmdfk
18	xppe xp lqepc esp ezrl alcej
19	wood wo kpdob dro dyqk zkbdi
20	vnnc vn jocna cqn cxpj yjach
21	ummb um inbmz bpm bwoi xizbg
22	tlla tl hmaly aol avnh whyaf
23	skkz sk glzkx znk zumg vgxze
24	rjjy rj fkyjw ymj ytlf ufwyd
25	qiix qi ejxiv xli xske tevxc

- Since there are only 25 possible keys, and only 26 letters of the alphabet, it is trivial to just try them all.

MONOALPHABETIC CIPHERS

- Permutation of a finite set S
- An ordered sequence of the elements of S , each one appearing exactly once
- If the cipher can be any permutation of the 26 alphabetic characters, then there are 26! or greater than 4×10^{26} possible keys
- This is 10 orders of magnitude greater than the key space for DES (2^{56})
- Called monoalphabetic substitution because a single cipher alphabet is used per message

MONOALPHABETIC CIPHER



Relative Frequency of Letters in English Text

MONOALPHABETIC CIPHER

- Easy to break because they reflect the frequency data of the original alphabet
- Countermeasure is to provide multiple substitutes (homophones) for a single letter
- Digrams
  - Two-letter combination
  - Most common is th
- Trigram
  - Three-letter combination
  - Most frequent is the

PLAYFAIR CIPHER

- Multiple-letter encryption cipher
- Treats digrams in the plaintext as single units and translates these units into ciphertext digrams
- Based on the use of a 5 x 5 matrix of letters constructed using a keyword
- Used as the standard field system by the British Army in World War I and the U.S. Army and other Allied forces during World War II

PLAYFAIR CIPHER

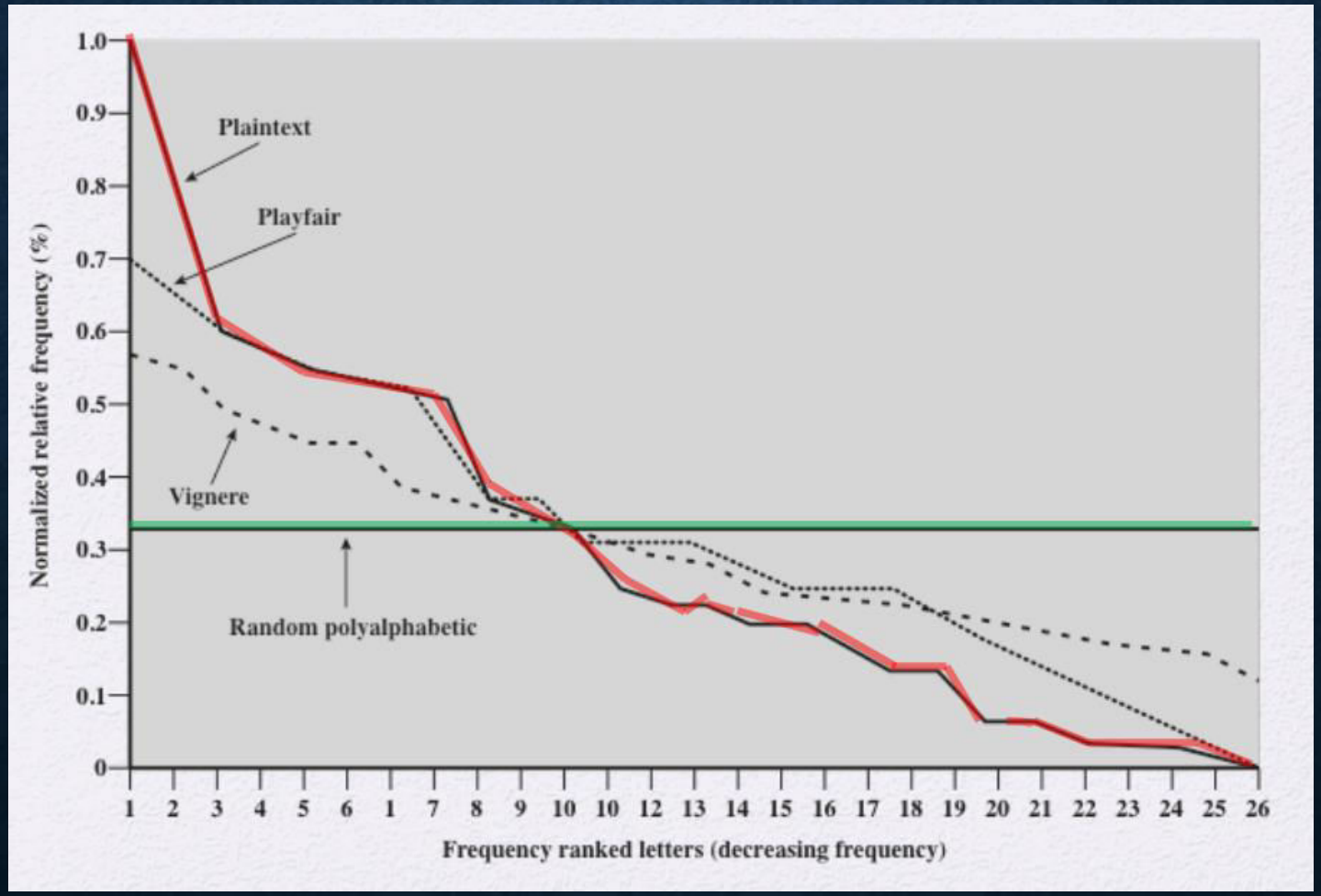
- Fill in letters of keyword (minus duplicates) from left to right and from top to bottom, then fill in the remainder of the matrix with the remaining letters in alphabetic order

- Keyword MONARCHY:

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

plaintext: H I D E C E
ciphertext: b f c k e l

FREQUENCY ANALYSIS



HILL CIPHER

- Developed by the mathematician Lester Hill in 1929
- Strength is that it completely hides single-letter frequencies
- The use of a larger matrix hides more frequency information
- A 3 x 3 Hill cipher hides not only single-letter but also two letter frequency information
- Strong against a ciphertext-only attack but easily broken with a known plaintext attack

HILL CIPHER

- plaintext: ACT
- key: GYBNQKURP
- Convert to vector and 3 x 3 matrix
- plaintext: (0 2 19) key: $\begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix}$
- ciphertext is: $\begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix} \begin{pmatrix} 0 \\ 2 \\ 19 \end{pmatrix} = \begin{pmatrix} 67 \\ 222 \\ 391 \end{pmatrix} = \begin{pmatrix} 15 \\ 14 \\ 7 \end{pmatrix} \bmod 26$
- Convert back to letters: p o h

POLYALPHABETIC CIPHERS

- Polyalphabetic substitution cipher
- Uses different monoalphabetic substitutions as one proceeds through the plaintext message
- All these techniques have the following features in common:
  - A set of related monoalphabetic substitution rules is used
  - A key determines which particular rule is chosen for a given transformation

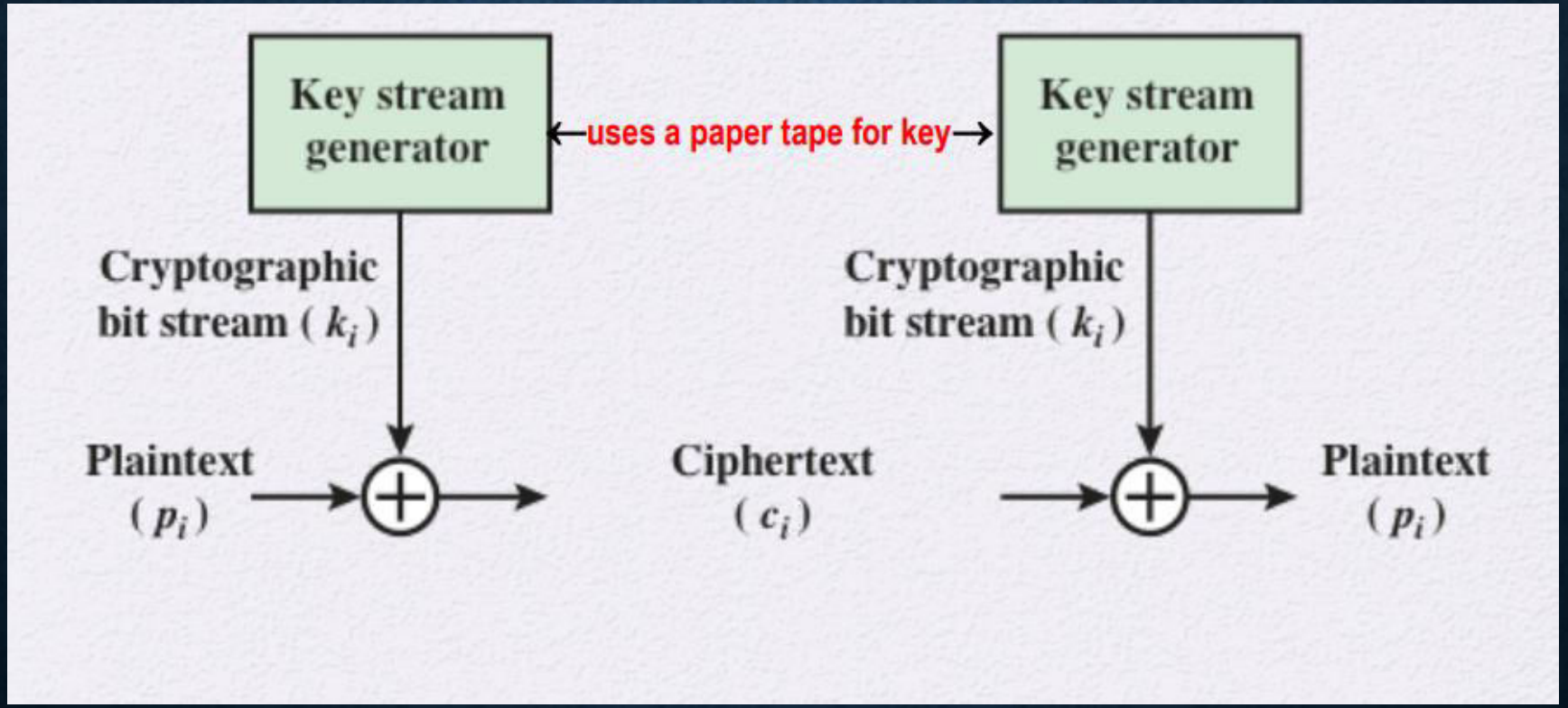
VIGENERE CIPHER

- Best known and one of the simplest polyalphabetic substitution ciphers
- The set of monoalphabetic substitution rules consists of the Caesar ciphers with shifts of 0 through 25
- Each cipher is denoted by a key letter which is the ciphertext letter that substitutes the plaintext letter a
- The key needs to be as long as the message
- Repeat the keyword if necesaary
- Example:
- keyword `D E C E P T I V E`
- `key:  D E C E P T I V E D E C E P T I V E D E C E P T I V E`
- `plaintext:  W E A R E D I S C O V E R E D S A V E Y O U R S E L F`
- `ciphertext:  z i c v t w q n g r z g v t w a v z h c q y g l m g y`

VIGENERE AUTOKEY SYSTEM

- The keyword is concatenated with the plaintext itself to provide a running key
- Example:
- key: D E C E P T I V E W E A R E D I S C O V E R E D S A V
- plaintext: W E A R E D I S C O V E R E D S A V E Y O U R S E L F
- ciphertext: z i c v t w q n g k z e i i g a s x s t s l v v w l a
- Even this scheme is vulnerable to cryptanalysis
- Because the key and the plaintext share the same frequency distribution of letters, a statistical technique can be applied

VERNAM CIPHER



ONE TIME PAD

- Improvement proposed by an Army Signal Corp officer, Joseph Mauborgne
- Use a random key that is as long as the message so that the key need not be repeated
- Key is used to encrypt and decrypt a single message and then is discarded
- Each new message requires a new key of the same length as the new message
- Scheme is unbreakable
  - Produces random output that bears no statistical relationship to the plaintext
  - Because the ciphertext contains no information whatsoever about the plaintext, there is simply no way to break the code

ONE TIME PAD - DIFFICULTIES

- The one-time pad offers unconditional security (perfect secrecy).
- However the distribution of random keys that are as long as the message to be sent is a fundamental key distribution problem
- Because of this, the one-time pad is of limited utility
- Uses primarily for low-bandwidth channels requiring very high security

RAIL FENCE CIPHER – TRANSPOSITIONAL CIPHER

- Transposition ciphers add diffusion
- Spread out the bits of the message in the ciphertext.
- Make the relationship between the plaintext and ciphertext complex.
- Plaintext is written down as a sequence of diagonals and then read off as a sequence of rows
- To encipher the message .“MEET ME AFTER THE TOGA PARTY” with a Rail Fence cipher of depth 2, we would write:

```
M e m a t r h t g p r y
  e t e f e t e o a a t
```

- Encrypted message is: mematrhtgpryetefeteoaat

ROW TRANSPOSITION CIPHER

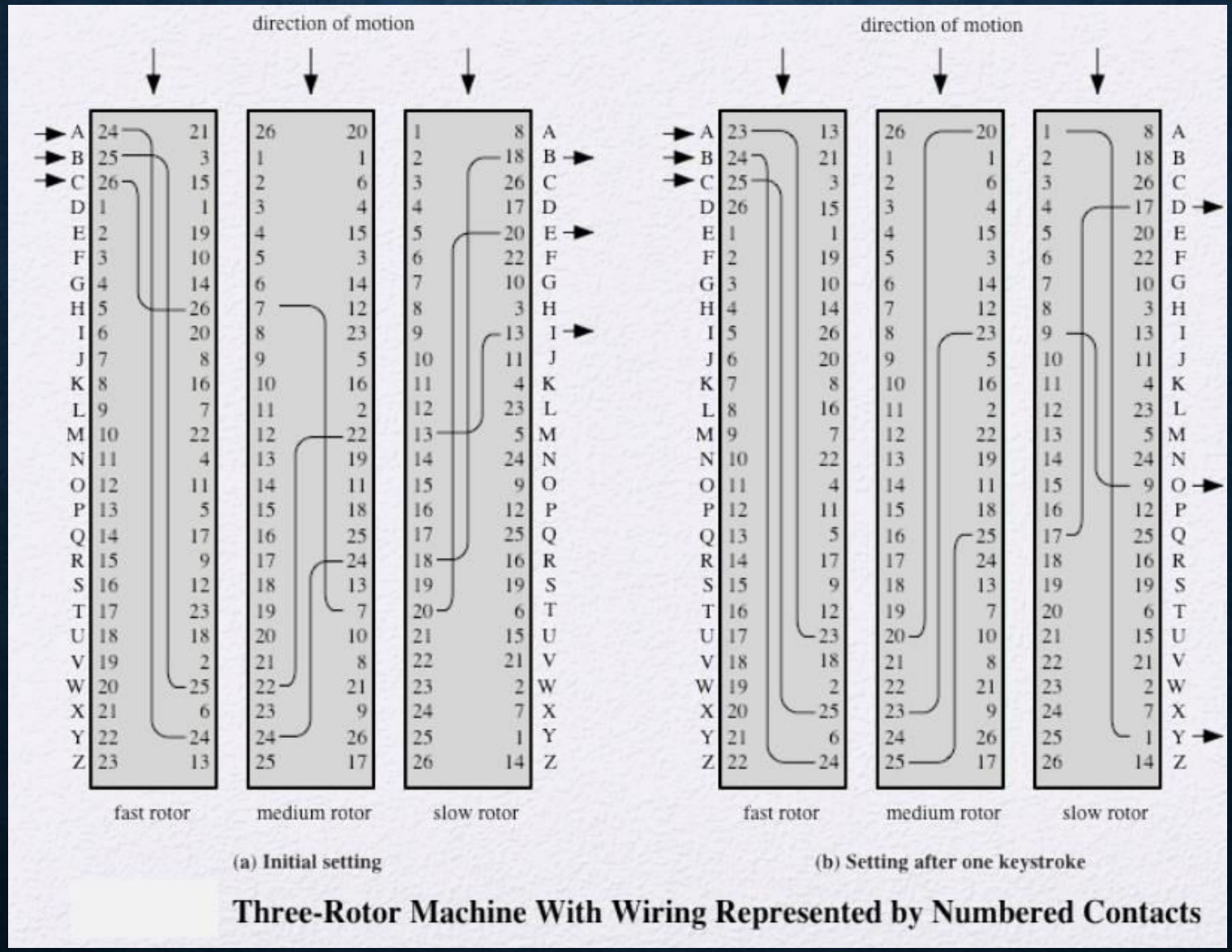
- A more complex transposition cipher
- Write the message in a rectangle, row by row, and read the message off, column by column, but permute the order of the columns
- The order of the columns then becomes the key to the algorithm

Key: 4 3 1 2 5 6 7

Plaintext:	A	T	T	A	C	K	P
	O	S	T	P	O	N	E
	D	U	N	T	I	L	T
	W	O	A	M	X	Y	Z

Ciphertext: ttnaaptmtsuoaodwcoixknlypetz

ROTOR MACHINE



Three-Rotor Machine With Wiring Represented by Numbered Contacts