NT219- Cryptography

Week 3: Modern Symmetric Ciphers

PhD. Ngoc-Tu Nguyen

tunn@uit.edu.vn

What is cryptograph?

- Cryptology= Cryptography + Cryptanalysis

What?

Goals

- Confidentiality
- Privacy

Cipher systems

- Sysmmetric (AES)

- Asymmetric (RSA, ECC, CRYSTALS-KYBER)

- Integrity
- Authentication

Hash functions

Message authentication code (MAC)

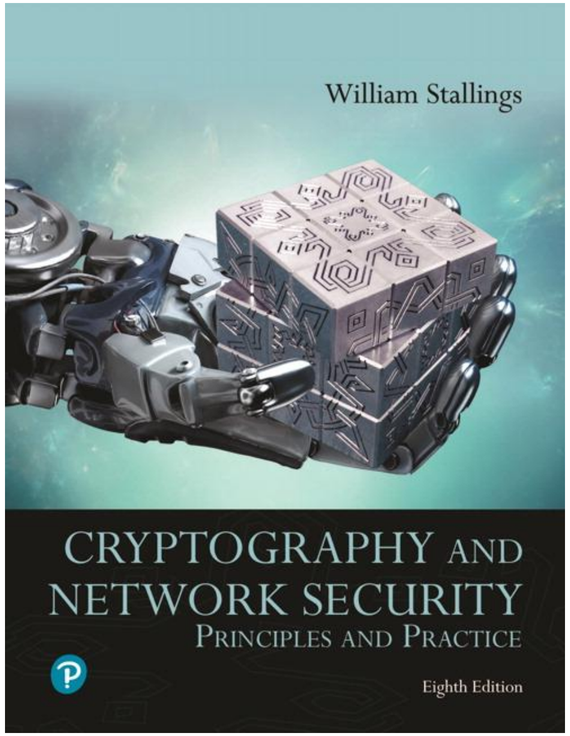
Digital signature (digital certificate)

- Non-repudiation (Accountability)

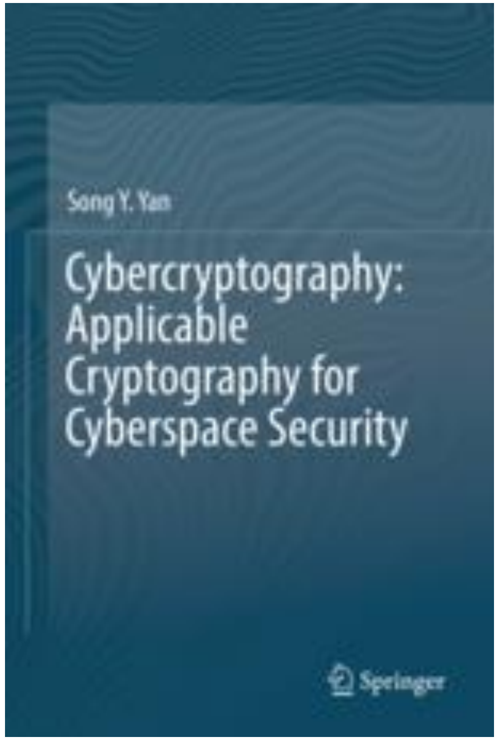
- Availability

Textbooks and References

- Text books



[1] Chapter 4,6



Song Y. Yan

Cybercryptography: Applicable Cryptography for Cyberspace Security

Springer

[2] Chapter 5

Classical cipher algorithms

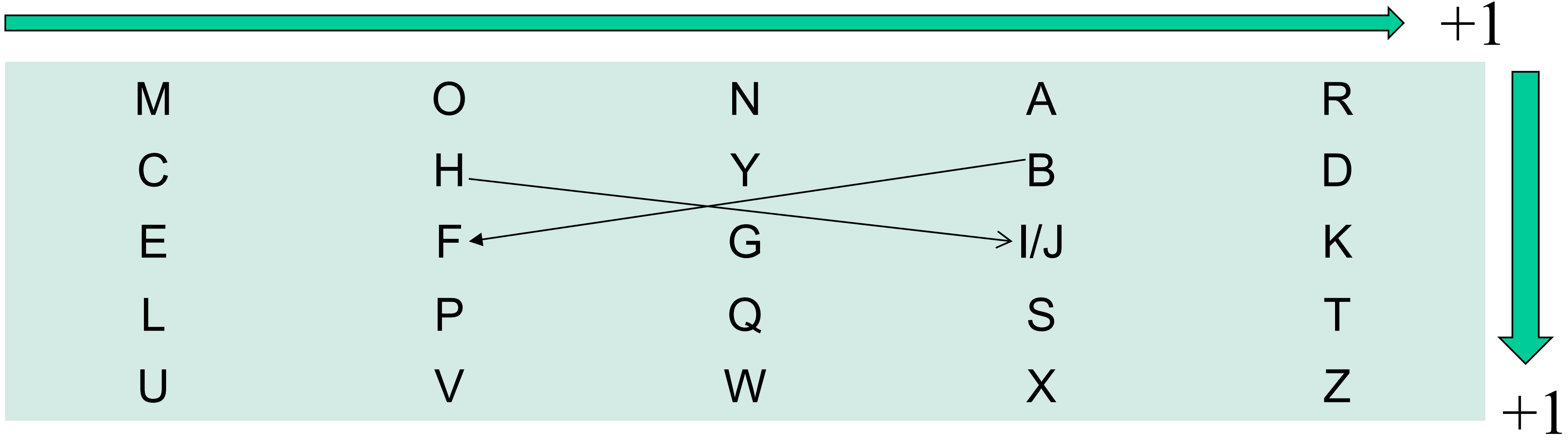
- **Substitution** Technique
  - Monoalphabetic cipher
    - Replace one character by another character
    - Replace one character by other characters
  - Polyalphabetic cipher
    - Replace some characters by other characters
      - 2 by 2:
      - 3 by 3 or n by n
- **Transposition** Technique
  - Keep the same source characters bat change their positions

Polyalphabetic Cipher

- Polyalphabetic Cipher: Replace some characters by other characters
  - **Playfair Cipher**: replace 2 characters by 2 characters
  - **Hill Cipher**: replace 3 characters by 3 characters, …
  - **Vigenère Cipher**

Playfair encryption

Key matrix



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: "Hide the gold in the tree stump"

Plaintext diagram:

HI DE TH EG OL DI NT HE TR EX ES TU MP

Ciphertext diagram:

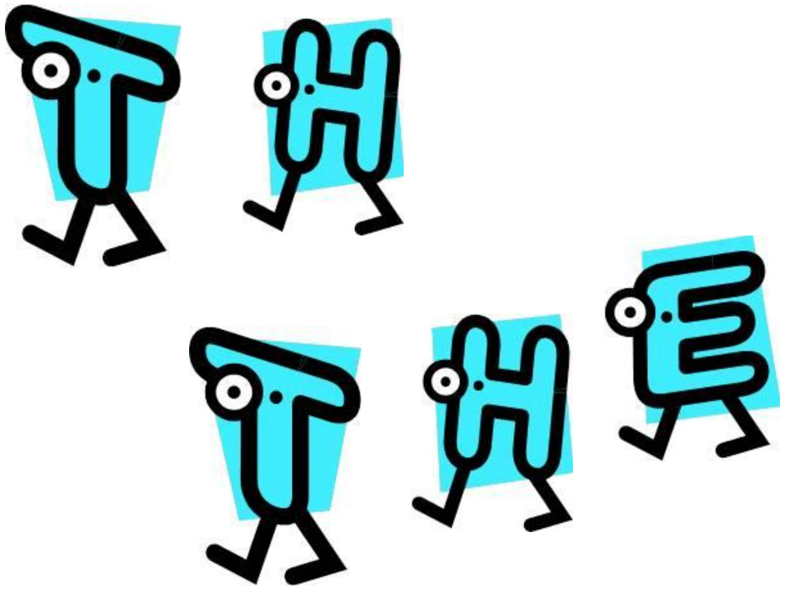
BF CK PD FI .. .. ZD

https://en.wikipedia.org/wiki/Playfair_cipher

Polyalphabetic Cipher

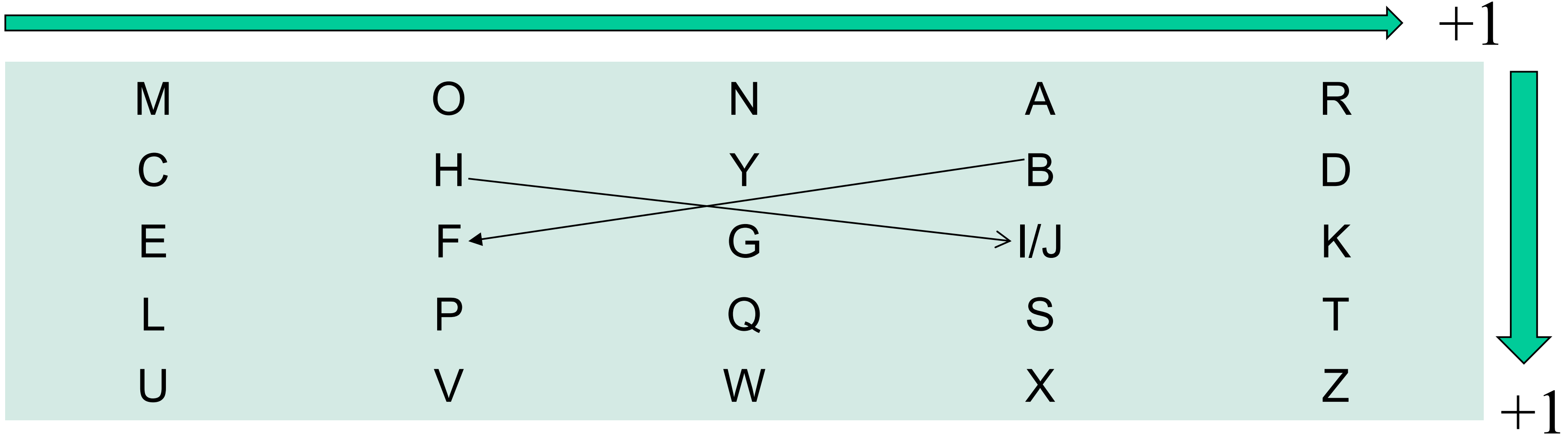
Cryptoanalys Playfair cipher

- Digram
  - Two-letter combination
  - Most common is *th*
- Trigram
  - Three-letter combination
  - Most frequent is *the*



Cryptanalysis Playfair

Guess the Key?



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

- **UnigramScorer**: Single letter frequences;

  https://en.wikipedia.org/wiki/Frequency_analysis
- **DigramScorer**: Bigram frequences

  https://en.wikipedia.org/wiki/Bigram
- **QuadgramScorer:** Trigram frequences

  https://en.wikipedia.org/wiki/Trigram

Polyalphabetic Cipher

(4) Hill Cipher

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
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

- 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

$$C = K.P \bmod 26$$

$$\begin{pmatrix} k_{1,1} & k_{1,2} & k_{1,3} \\ k_{2,1} & k_{2,2} & k_{2,3} \\ k_{3,1} & k_{3,2} & k_{3,3} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} c_1 \\ c_2 \\ c_3 \end{pmatrix} \bmod 26$$

Polyalphabetic Cipher

(5) Vigenère Cipher

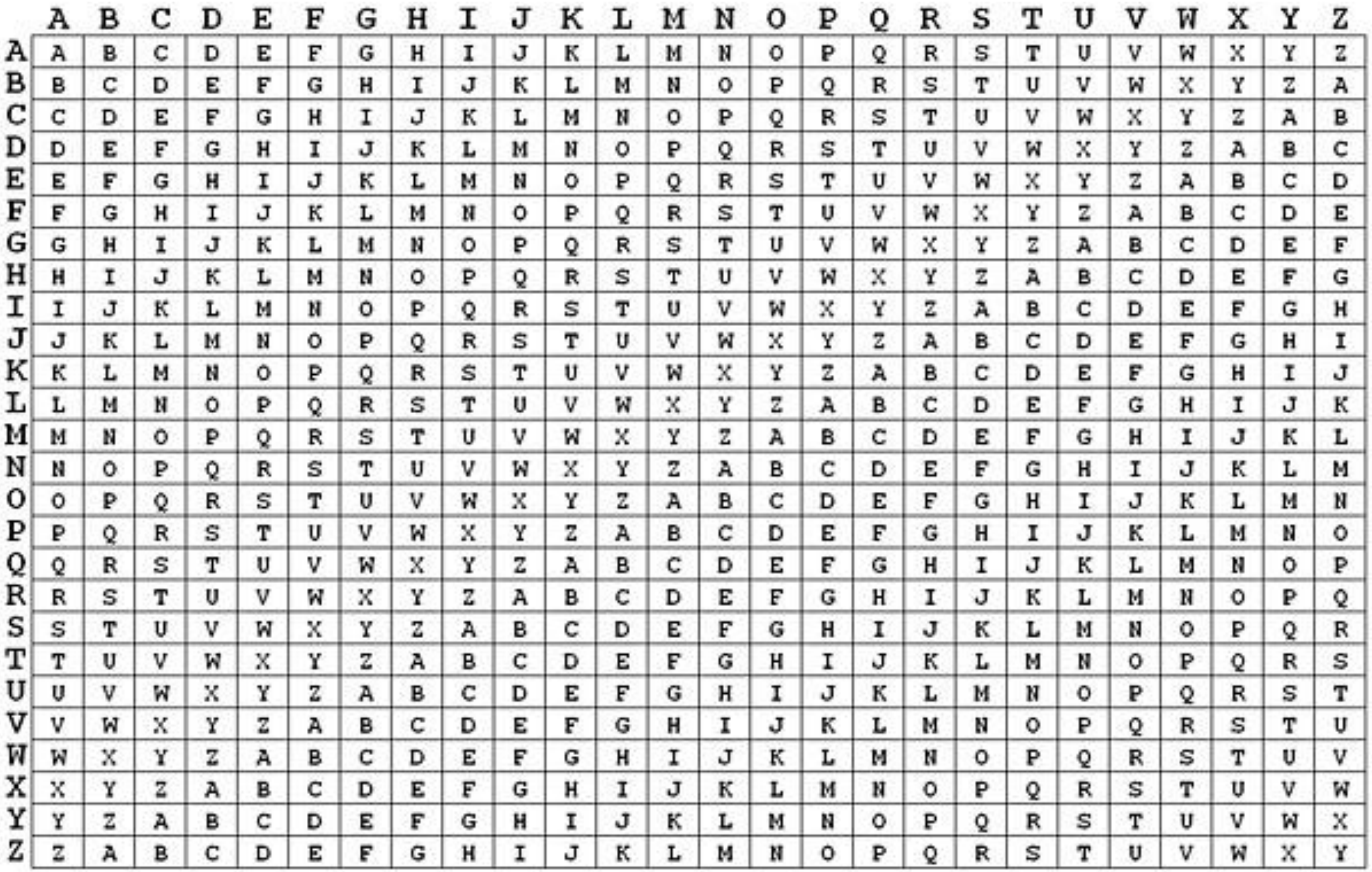
- Best known and one of the simplest polyalphabetic substitution ciphers
- In this scheme the set of related monoalphabetic substitution rules consists of the 26 Caesar ciphers with shifts of 0 through 25
- Each cipher is denoted by a key letter which is the ciphertext letter that substitutes for the plaintext letter a

https://en.wikipedia.org/wiki/Vigen%C3%A8re_cipher

Vigenère Cipher

- Vigenère matrix

Key: deceptiv



		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
3	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
1	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
2, 4	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
7	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
5	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
6	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
8	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

Example of Vigenère Cipher

- To encrypt a message, a key is needed that is as long as the message
- Usually, the key is a repeating keyword
- For example, if the keyword is *deceptive*, the message “we are discovered save yourself” is encrypted as:

key:	deceptivedeceptivedeceptive
plaintext:	wearediscoveredsaveyourself
ciphertext:	??

Vigenère Autokey System

- Example:

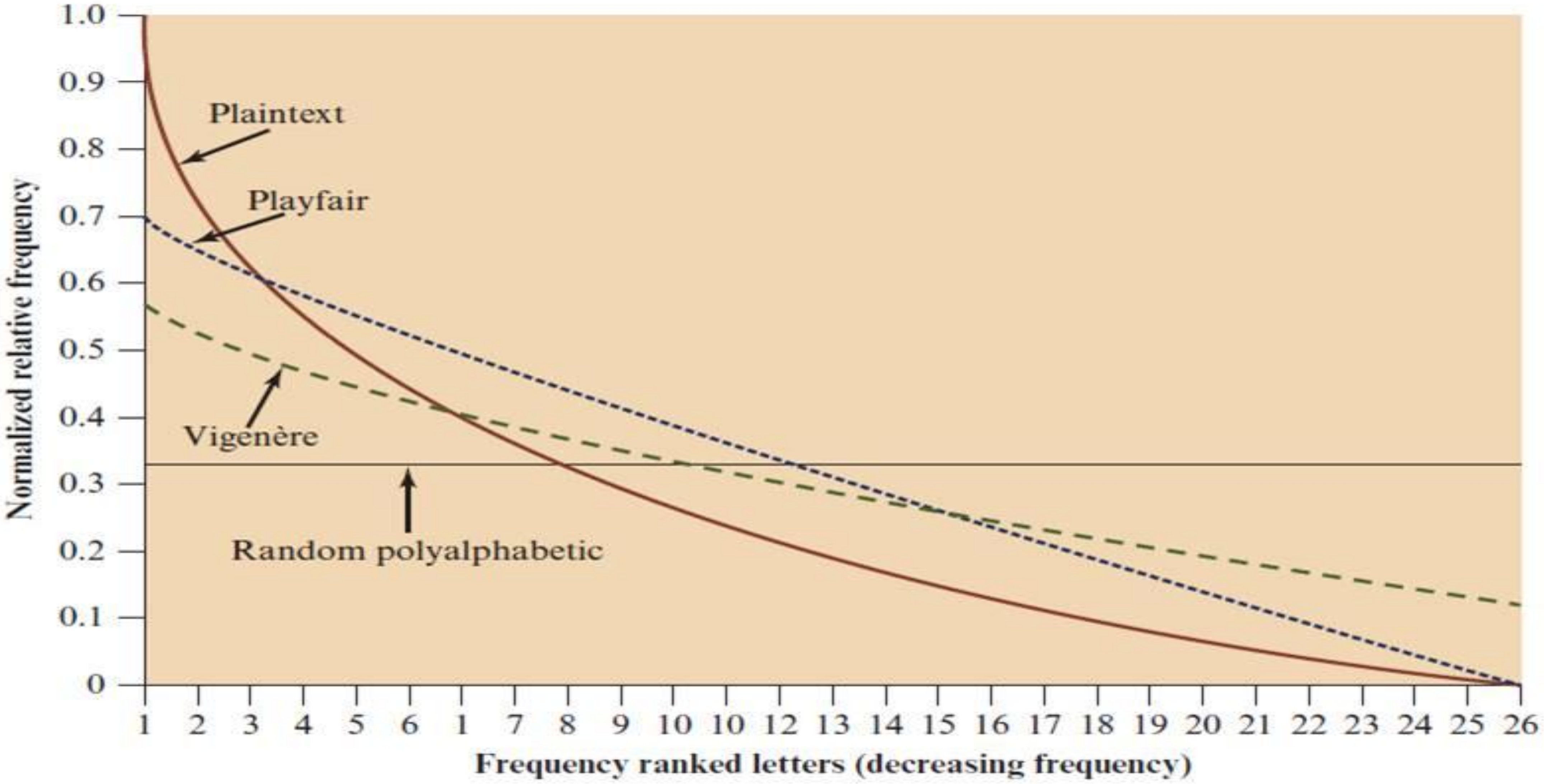
  plaintext: w e a r e d i s coveredsaveyourself

  key: d e c e p t I v eweare discoveredsav

  ciphertext: ZICVTWQNGKZEIIGASXSTSLVVWLA

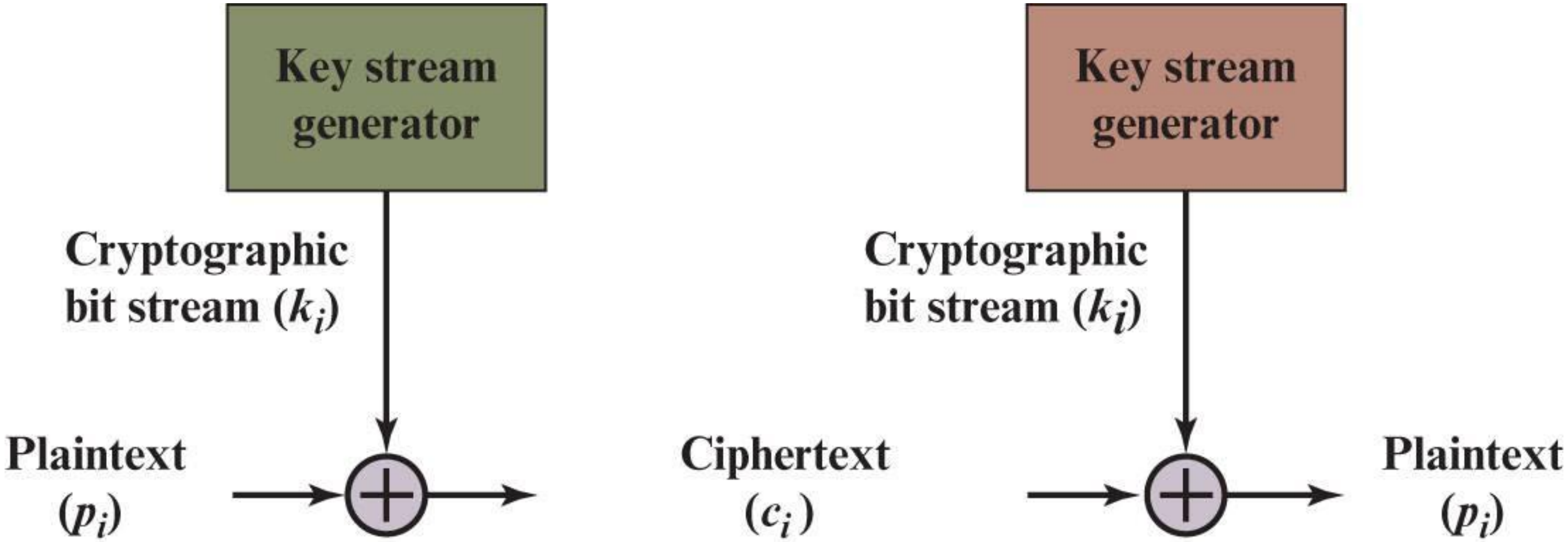
- Even this scheme is vulnerable to cryptanalysis
  - ➢ Because the key and the plaintext share the same frequency distribution of letters, a statistical technique can be applied

Classical symmetric cipher cryptanalysis



Stream ciper

(6) Vernam Cipher



https://en.wikipedia.org/wiki/Gilbert_Vernam

One-Time Pad

- Improvement to Vernam cipher 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

Difficulties

- The one-time pad offers complete security but, in practice, has two fundamental difficulties:
  - There is the practical problem of making large quantities of random keys
    - Any heavily used system might require millions of random characters on a regular basis
  - Mammoth key distribution problem
    - For every message to be sent, a key of equal length is needed by both sender and receiver
- Because of these difficulties, the one-time pad is of limited utility
  - Useful primarily for low-bandwidth channels requiring very high security
- The one-time pad is the only cryptosystem that exhibits *perfect secrecy* (see Appendix F)

Transposition ciphers (permutation cipher)

Goals: scrambles the positions of characters

(1) Rail fence cipher

(2) Columnar Transposition Cipher

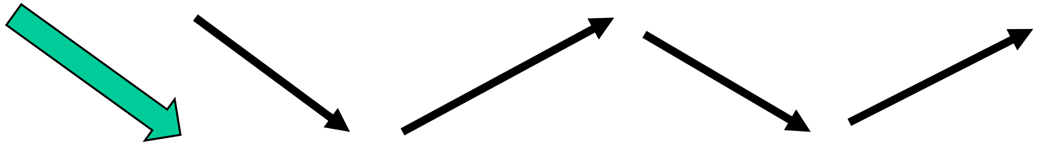
(3)

https://en.wikipedia.org/wiki/Transposition_cipher

Transposition cipher

(1) Rail fence cipher

- Simplest transposition cipher
- 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 of depth 2, we would write:



Ciphertext

Encrypted message is:

MEMATRHTGPRYETEFETEOAAT

https://en.wikipedia.org/wiki/Rail_fence_cipher

Columnar Transposition Cipher

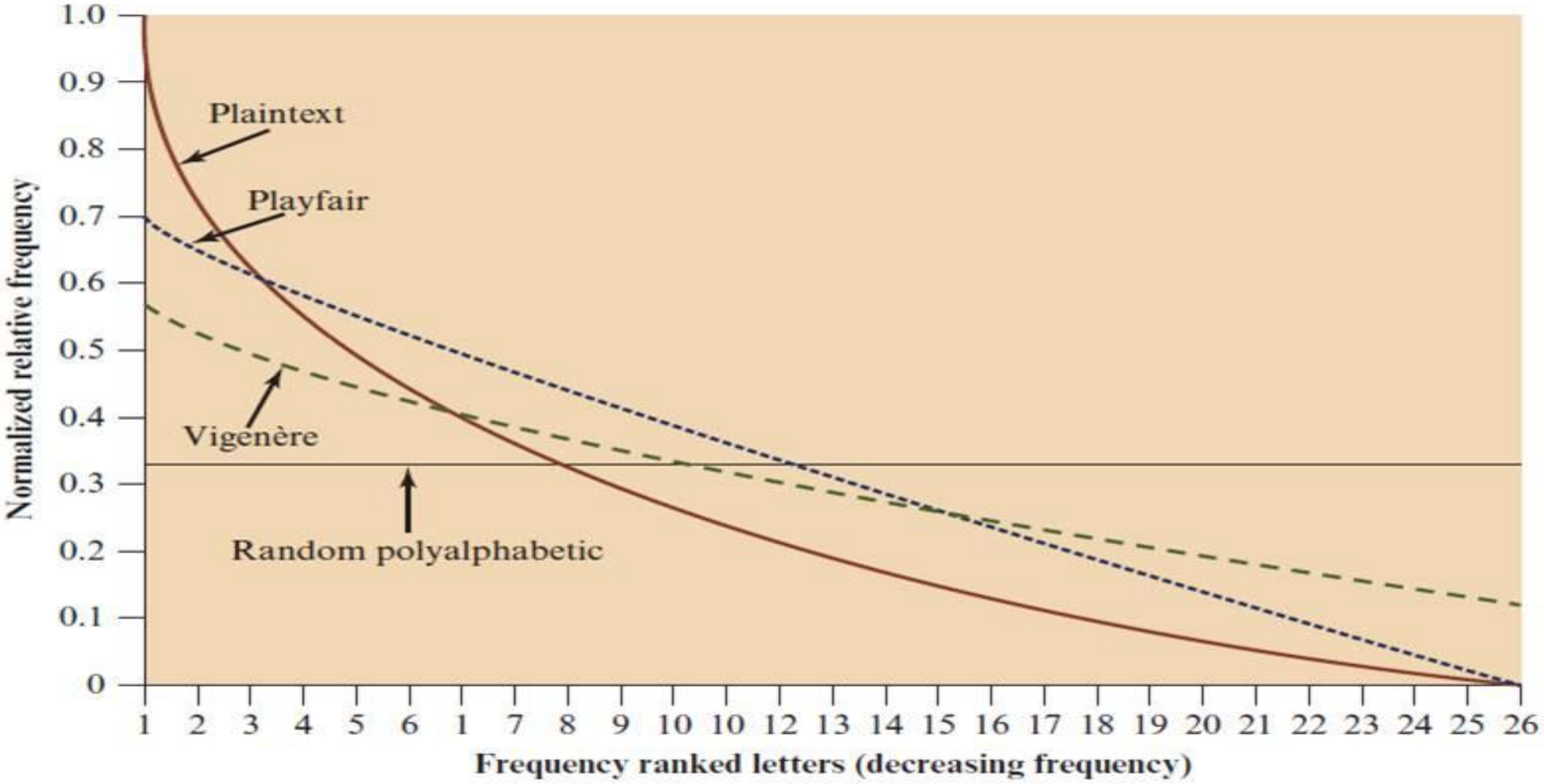
- Is a more complex transposition
- Write the message in a rectangle, row by row, and read the message off, column by column, but permute the order of the columns
  - The order of the columns then becomes the key to the algorithm

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

Ciphertext: TTNAAPTMTSUOAODWCOIXKNLYPETZ

Classical symmetric cipher cryptanalysis



Stream Cipher (1 of 8)

Vigenère cipher

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

- **Plaintext stream**

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

- **Secret key (Keystream)**

K'	=	L	E	M	O	N	L	E	M	O	N	L	E
		11	4	12	14	13	11	4	12	14	13	11	4

➢ **Ciphertext**

C	=	L	X	F	O	P	V	E	F	R	N	H	R
		11	23	5	14	15	21	4	5	17	13	7	17

$C = c_1 c_2 \cdots c_i \cdots$ where $c_i = m_i + k_i \bmod 26$

Stream Cipher (2 of 8)

- **Secret key (Keystream)**

$$K = k_1 k_2 \cdots k_i \cdots$$

- **Plaintext stream**

$$M = m_1 m_2 \cdots m_i \cdots$$

m_i : bit or byte

➢ **Ciphertext**

$$C = c_1 c_2 \cdots c_i \cdots$$

where $c_i = m_i \overline{\oplus} k_i$

$$k1 \quad k2 \quad k3 \quad \ldots \quad k_n$$

$$m1 \quad m2 \quad m3 \quad \ldots \quad m_n$$

$$k1 \oplus m1 \quad k2 \oplus m2 \quad \ldots \quad k_n \oplus m_n$$

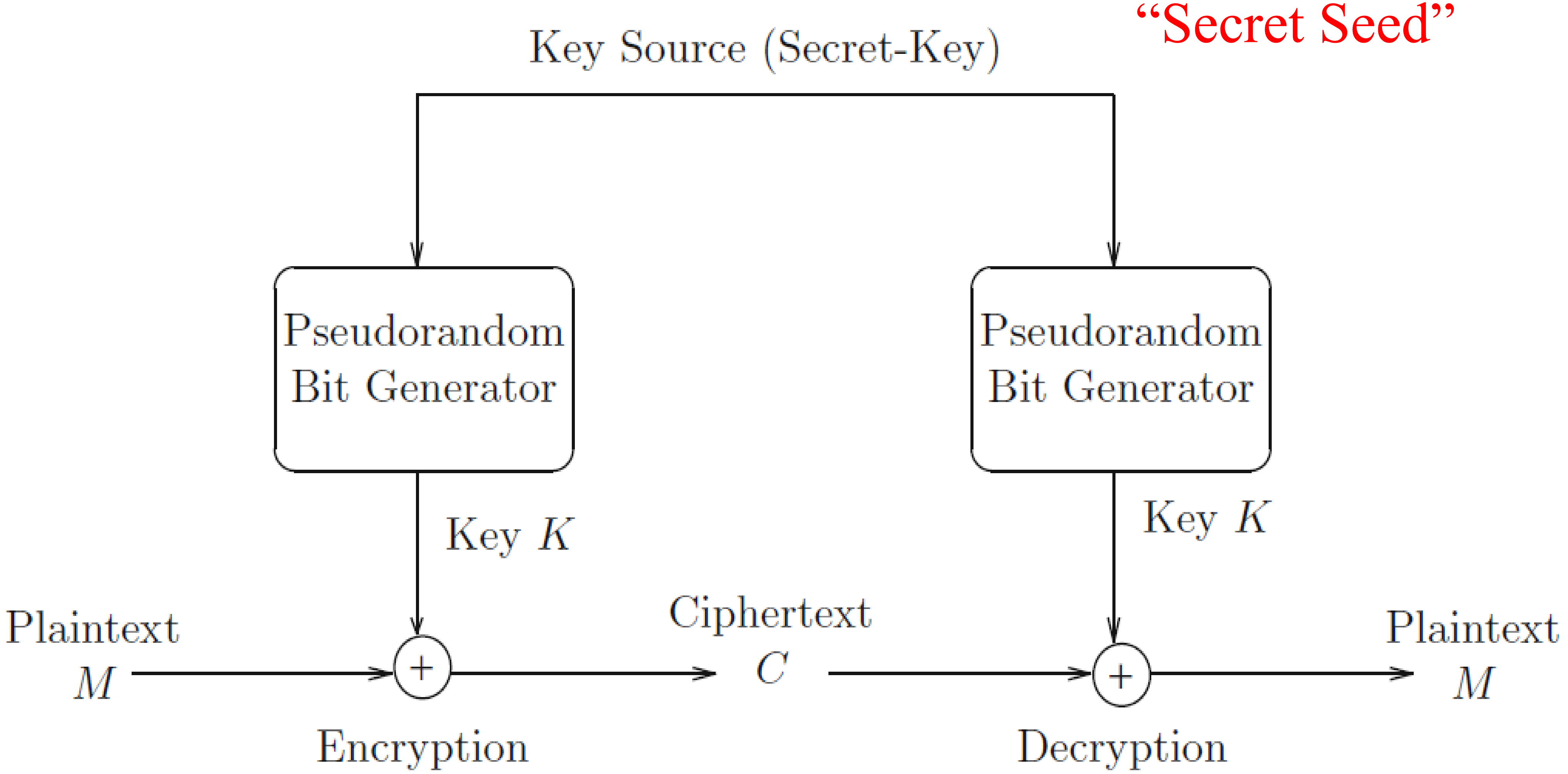
Stream Cipher (3 of 8)

- Encrypts a digital data stream **one bit or one byte** at a time
  - Examples:
    - **Autokeyed** Vigenère cipher
    - Vernam cipher
- In the ideal case, a one-time pad version of the Vernam cipher would be used, in which the keystream is as long as the plaintext bit stream
  - If the cryptographic keystream is random, then this cipher is unbreakable by any means other than acquiring the keystream
    - Keystream must be provided to both users in advance via some independent and secure channel
    - This introduces insurmountable logistical problems if the intended data traffic is very large

Stream Cipher (4 of 8)

- For practical: must be implemented as an algorithmic to **generate key bit stream** (both users)
  - It must be computationally impractical to predict future portions of the bit stream based on previous portions of the bit stream
  - The two users need only share the generating key and each can produce the keystream

Stream Cipher (5 of 8)



"Secret Seed"

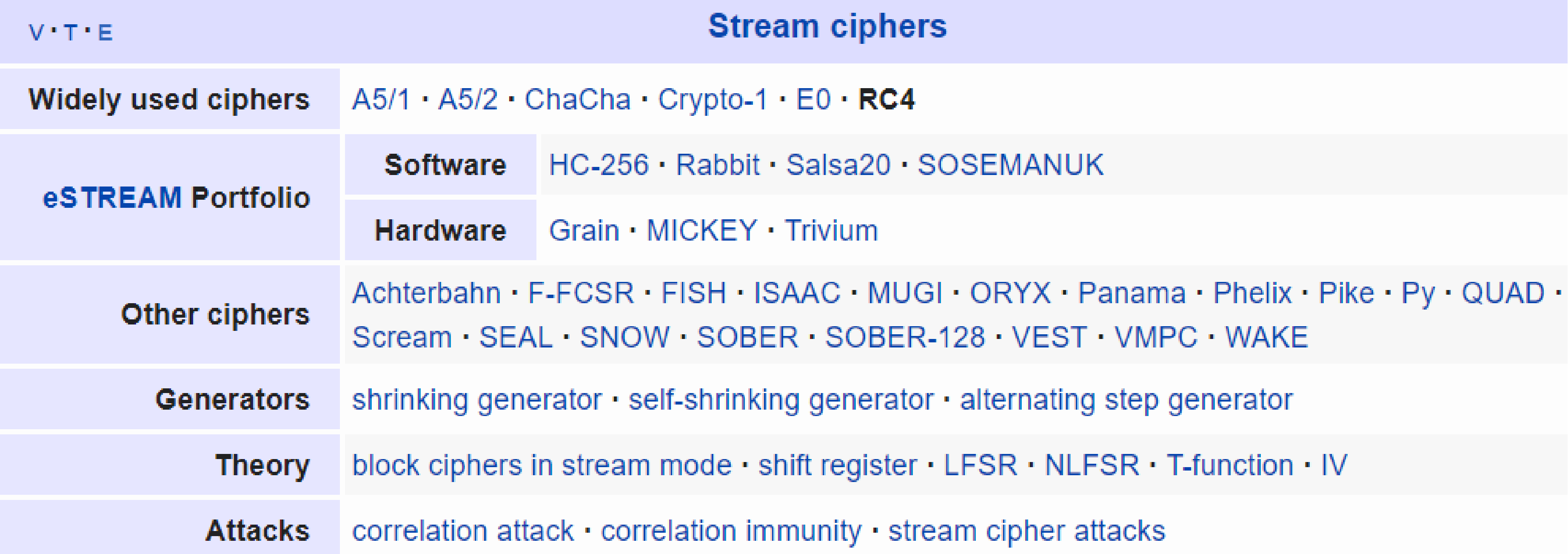
Stream Cipher (6 of 8)

- ➢ **Rivest Cipher 4**

https://en.wikipedia.org/wiki/RC4

- ➢ **Chaotic-based cryptosystem**

https://en.wikipedia.org/wiki/List_of_chaotic_maps



V · T · E	Stream ciphers	
Widely used ciphers	A5/1 · A5/2 · ChaCha · Crypto-1 · E0 · **RC4**	
eSTREAM Portfolio	**Software**	HC-256 · Rabbit · Salsa20 · SOSEMANUK
	Hardware	Grain · MICKEY · Trivium
Other ciphers	Achterbahn · F-FCSR · FISH · ISAAC · MUGI · ORYX · Panama · Phelix · Pike · Py · QUAD · Scream · SEAL · SNOW · SOBER · SOBER-128 · VEST · VMPC · WAKE	
Generators	shrinking generator · self-shrinking generator · alternating step generator	
Theory	block ciphers in stream mode · shift register · LFSR · NLFSR · T-function · IV	
Attacks	correlation attack · correlation immunity · stream cipher attacks	

Stream Cipher (7 of 8)

- **Chaotic-based cryptosystem**

Example:

Logistic map

$$x_{n+1} = rx_n(1 - x_n)$$

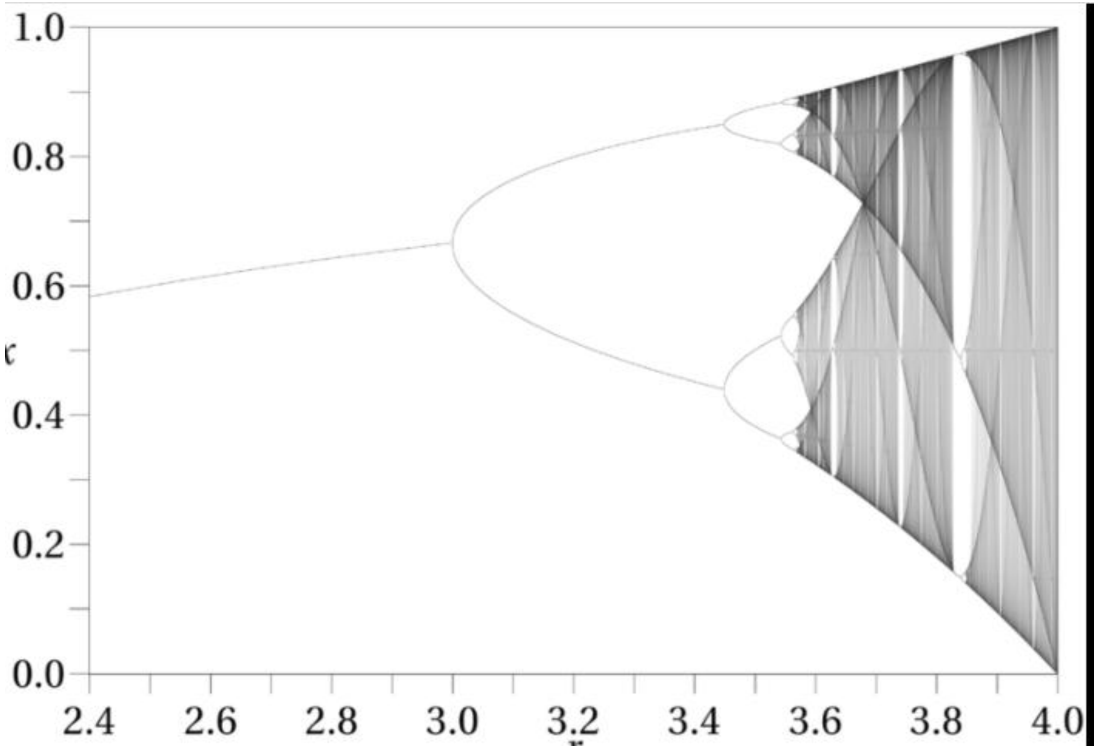
Input (seed):

$x_0, r \in (3.6, 4)$

Output:

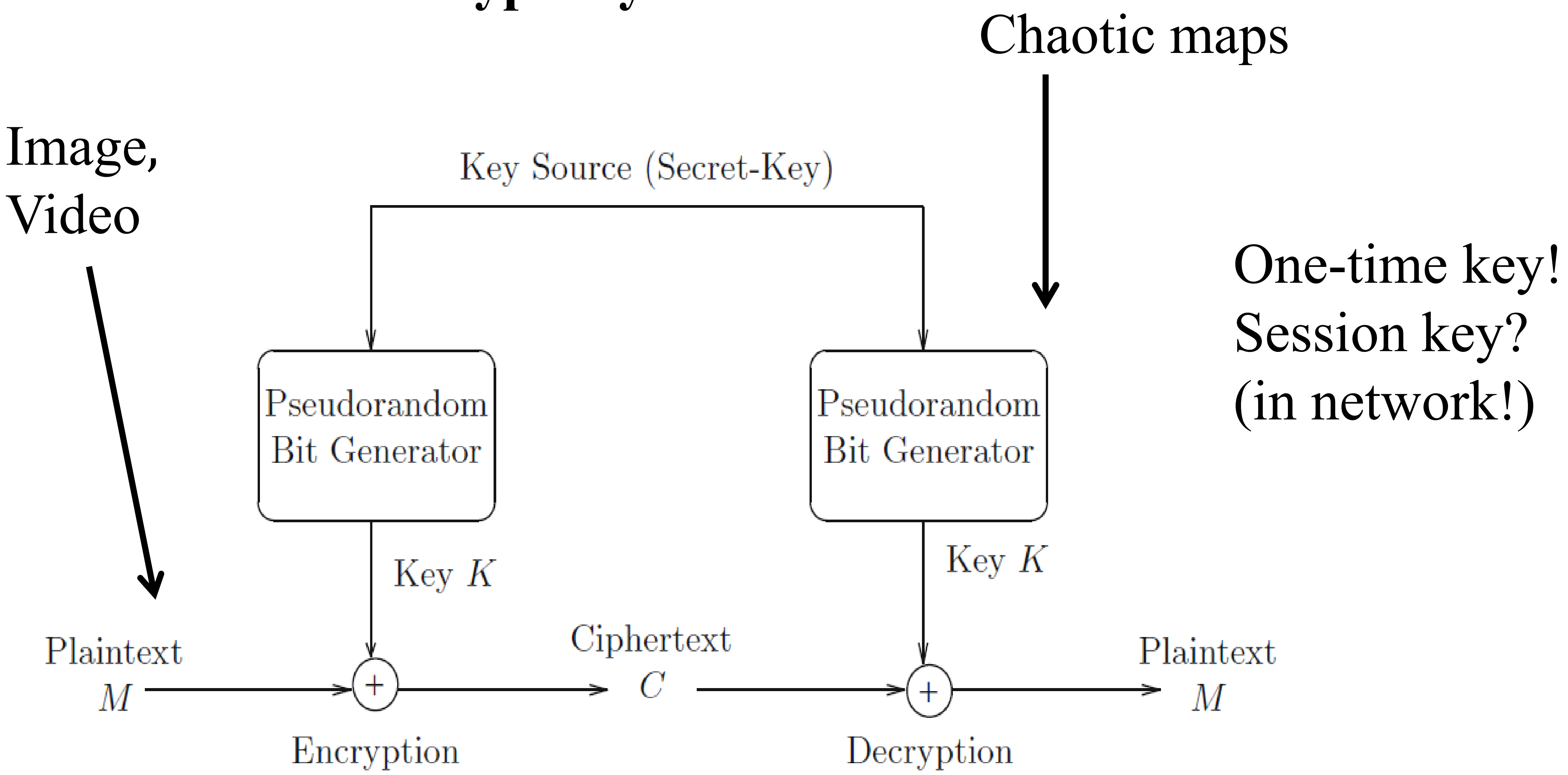
$$x_1, x_2, x_3, \dots x_n, \dots.$$

$$0 < x_i < 1$$



Stream Cipher (8 of 8)

- **Chaotic-based crypto system**



Outline (week 4,5)

- Stream Cipher
- Block cipher
  - Data Encryption Standard (DES)
  - Advanced Encryption Standard (AES)
  - Some other ciphers
    - Searchable encryption