THE UNIVERSITY OF BRITISH COLUMBIA

Introduction to Cryptography

EECE 412

Module Outline

- Historical background
  - Classic ciphers
  - One-time pad
- The Random Oracle model
  - Random functions: Hash functions
  - Random generators: stream ciphers
  - Random Permutations: block ciphers

learning objectives

- explain classic ciphers covered in the lectures
- encrypt and decrypt using these classic cyphers
- break classic ciphers (home assignment #2)
- explain one-time-pad and encrypt/decrypt wit it
- explain the Random Oracle Models for hash function, stream cipher, and block cipher

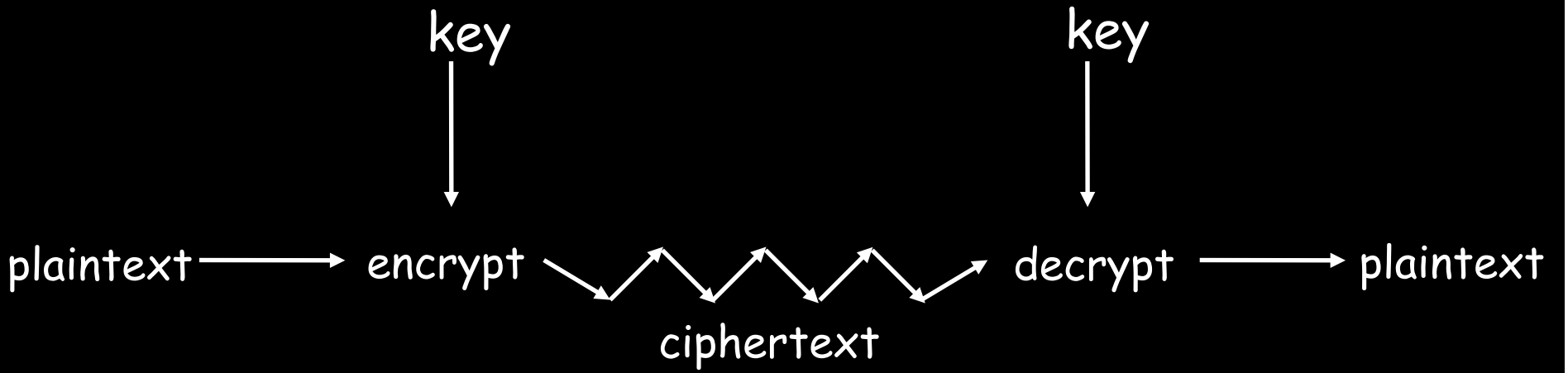
Crypto

- **Cryptology** — The art and science of making and breaking "secret codes"
- **Cryptography** — making "secret codes"
- **Cryptanalysis** — breaking "secret codes"
- **Crypto** — all of the above (and more)

How to Speak Crypto

- A *cipher* or *cryptosystem* is used to *encrypt* the *plaintext*
- The result of encryption is *ciphertext*
- We *decrypt* ciphertext to recover plaintext
- A *key* is used to configure a cryptosystem
- A *symmetric key* cryptosystem uses the same key to encrypt as to decrypt
- A *public key* cryptosystem uses a *public key* to encrypt and a *private key* to decrypt

Crypto as Black Box



A generic use of crypto

basic assumptions in crypto

- assumptions
  1. The system is completely known to the attacker
  2. Only the key is secret
- Also known as **Kerckhoffs Principle**
  - Crypto algorithms are not secret

Kerckhoff's Principle

"The security of a cryptosystem must not depend on keeping secret the crypto-algorithm. The security depends only on keeping secret the key"

Auguste Kerckhoff von Nieuwenhof

Dutch linguist

1883

basic assumptions in crypto

- assumptions
  1. The system is completely known to the attacker
  2. Only the key is secret
- Also known as **Kerckhoffs Principle**
  - Crypto algorithms are not secret
- Why do we make this assumption?
  - Experience has shown that secret algorithms are weak when exposed
  - Secret algorithms never remain secret
  - Better to find weaknesses beforehand

Historical Background

To read:

All of chapter 2
except 2.3.6 & 2.3.8, which are
optional reading

two types of ciphers

- substitution
- transposition

Letter Indices in English Alphabet

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	z
13	14	15	16	17	18	19	20	21	22	23	24	25

Caesar Cipher

- Plaintext is `HELLO WORLD`
- Change each letter to the third letter following it (X goes to A, Y to B, Z to C)
  - Key is 3, usually written as letter 'D'
  - **C = P + K mod 26**
- Ciphertext: `KHOOR ZRUOG`

```
Plain   HELLOWORLD
Key     DDDDDDDDDD
Cipher  KHOORZRUOG
```

a simple attack

- how to attack Caesar Cipher?
- exhaustive/brute-force (key) search
- with 26 keys, how many attempts on average?
- Trudy can try 2^{40} candidates/second
- 2^{56} -- 18 hours
- 2^{64} -- 6 months
- how to increase key space for substitution cipher?

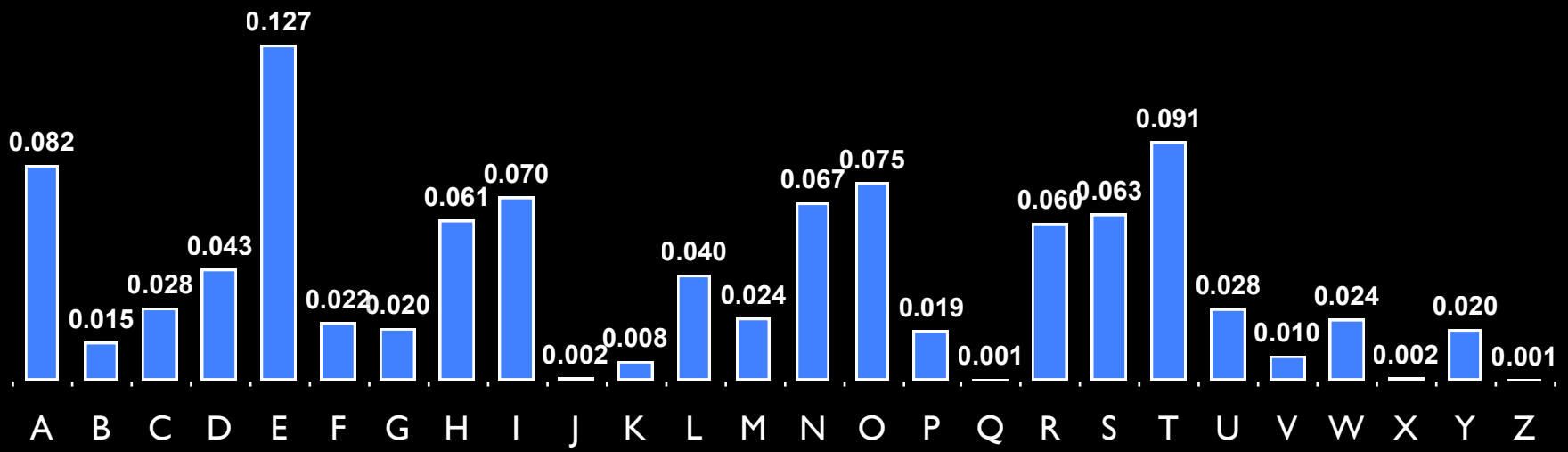
Monoalphabetic Substitution Cipher

Invented by Arabs in 8th or 9th centuries

A	B	C	D	E	F	G	H	I	J	K	L	M	N	..	Z
F	T	W	S	G	M	P	A	Z	C	L	V	O	D	..	B

```
Plain   HELLOWORLD
Key
Cipher  AGVVYEYZVS
```

Frequency Analysis of English Letters



Polyalphabetic Vigenère Cipher

proposed by Blaise de Vigenere from the court of Henry III of France in the sixteenth century

Like Cæsar cipher, but use a phrase

- Example
  - Message: TO BE OR NOT TO BE THAT IS THE QUESTION
  - Key: RELATIONS
  - Encipher using Cæsar cipher for each letter:

```
Plain   TO BE OR NOT TO BE TH AT I S THE QUESTION
Key     RE LA T I ONS RE LA T I ON SR ELA T I ONSREL
Cipher  KS ME HZ BBL KS ME MPOG AJ XSE J CSF LZSY
```

Playfair Cipher

background

- encrypts pairs of letters (digraphs), instead of single letters
  - ~600 possible digraphs rather than the 26 possible monographs
- was used for tactical purposes by
  - British forces in the Second Boer War (in South Africa) and in World War I
  - the Australians and Germans during World War II

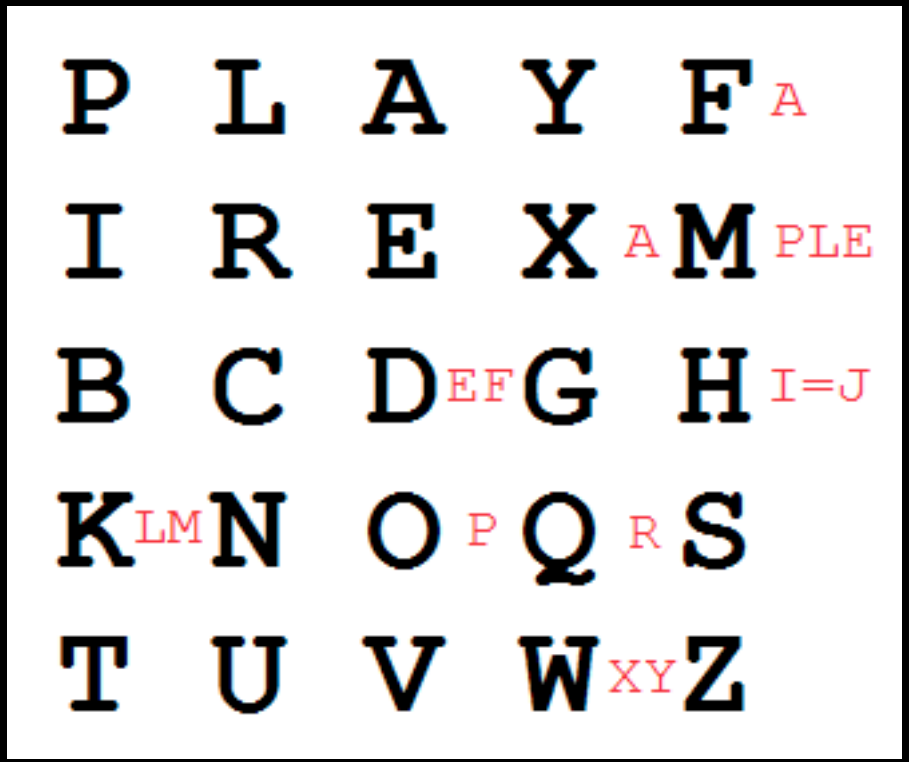
anecdotal history

source: wikipedia.org

- invented in 1854 by Charles Wheatstone
- rejected by the British Foreign Office when it was developed because of its perceived complexity
- Wheatstone offered to demonstrate that three out of four boys in a nearby school could learn to use it in 15 minutes
- the Under Secretary of the Foreign Office responded: "That is very possible, but you could never teach it to attachés."
- named after Lord Playfair who promoted the use of the cipher

setting up the cipher

- 5 x 5 table
- key example:
  “playfair example”
- drop any duplicate letters
- fill the remaining of the letters from English the alphabet / one letter (J or Q)



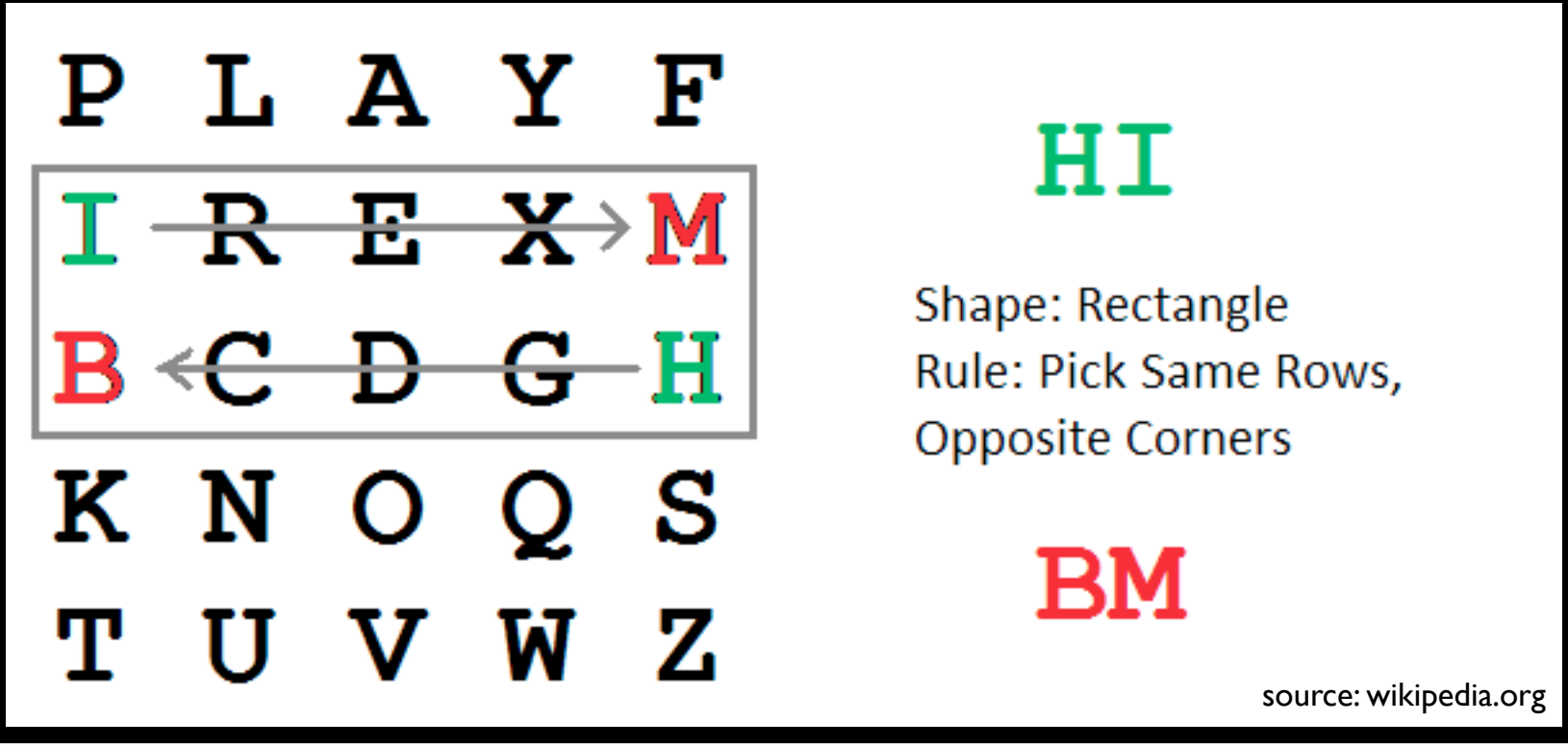
source: wikipedia.org

encryption overview

1. break the plain text into digraphs
   1. append “X” if odd number of characters.
   2. split double letters with “X”, e.g., “EE” -> “EXE”
   3. "Hide the gold in the tree stump" becomes "HI DE TH EG OL DI NT HE TR EX ES TU MP"
2. map each digraph out using the table

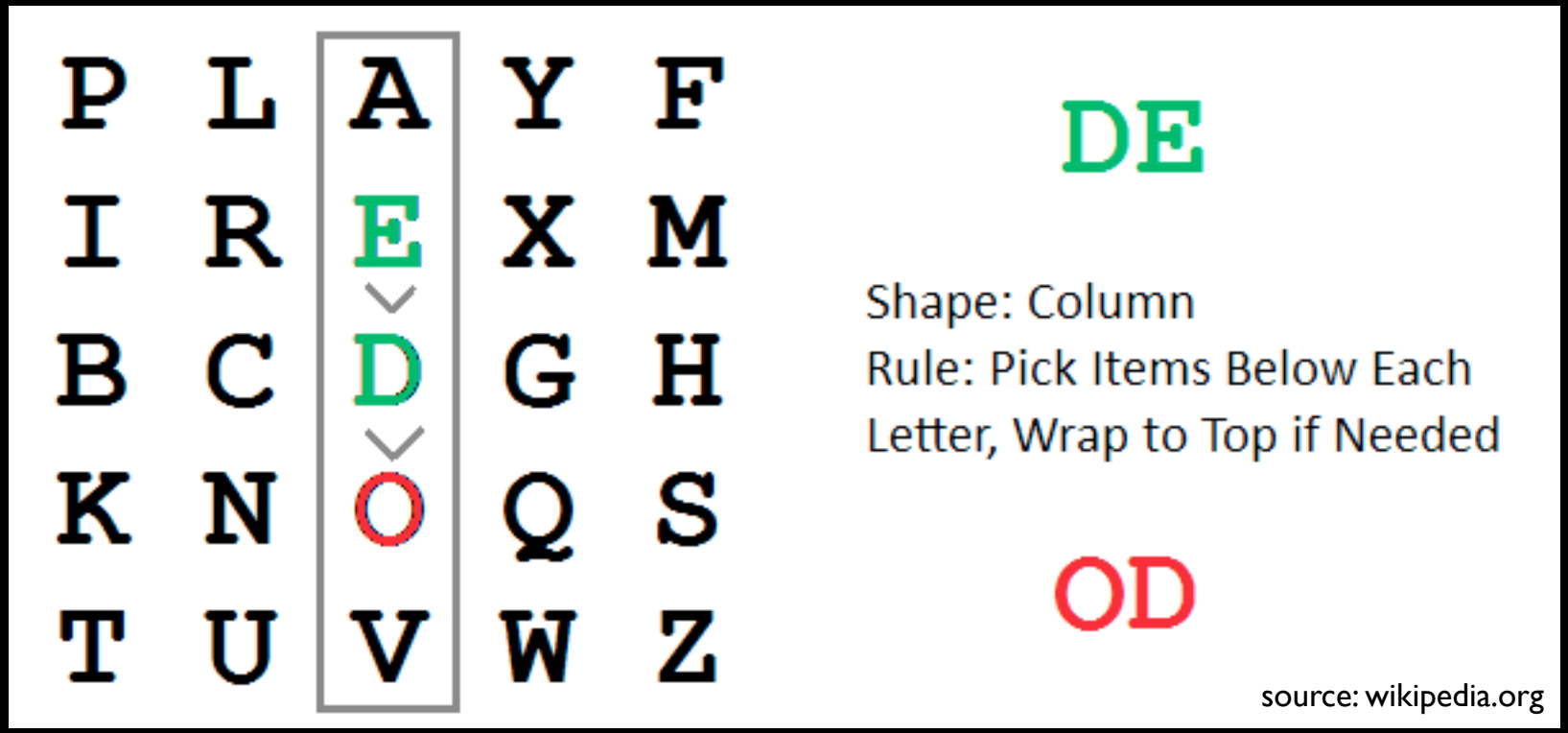
mapping rules

If a pair forms a rectangle, replace it with letters from the opposite corners on the same row.



mapping rules

If the letters appear on the same column of your table, replace them with the letters immediately below respectively.



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

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

“BM OD ? ? ...

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

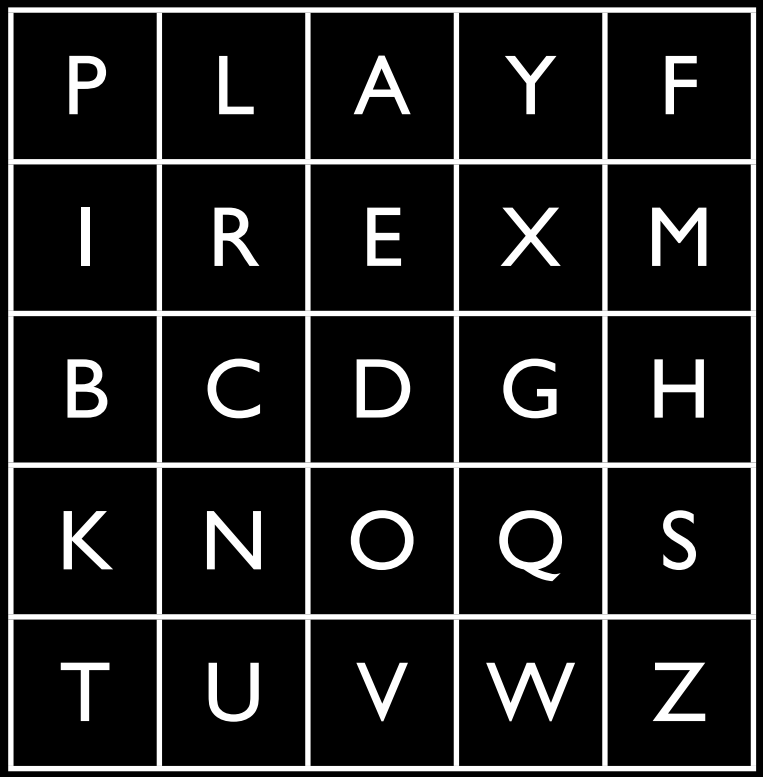
“HI DE TH EG OL DI NT HE TR EX ES TU MP”

“BM OD ZB ? ? ...

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

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

“BM OD ZB XD ? ? ...



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

“BM OD ZB XD NA ?? ...

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

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

“BM OD ZB XD NA BE ? ? ...

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

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

“BM OD ZB XD NA BE KU ? ? ...

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

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

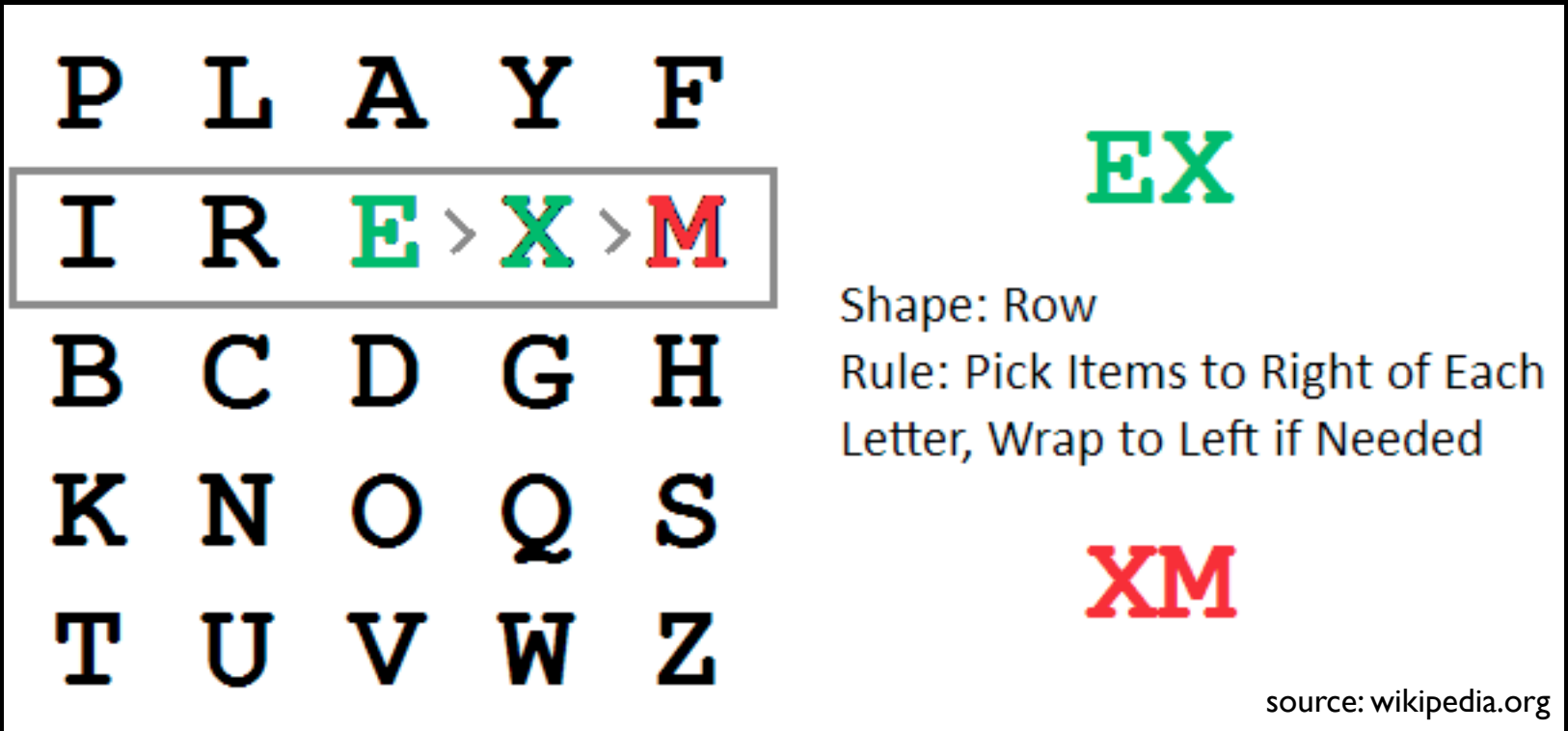
“BM OD ZB XD NA BE KU DM ? ? ...

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

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

“BM OD ZB XD NA BE KU DM UI ? ? ...

If the letters appear on the same row of your table, replace them with the letters immediately to right, respectively. Wrap to left, if needed.



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

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

“BM OD ZB XD NA BE KU DM UI XM ? ? ...

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

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

“BM OD ZB XD NA BE KU DM UI XM MO ? ? ...

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

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

“BM OD ZB XD NA BE KU DM UI XM MO UV ? ? ...

"HIDE THE GOLD IN THE TREE STUMP"

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

"BM OD ZB XD NA BE KU DM UI XM MO UV IF"

- How to decrypt it with the key?
- What betrays Palyfair?
- How can one break it?

Double Transposition

	col 1	col 2	col 3
row 1	a	t	t
row 2	a	c	k
row 3	x	a	t
row 4	x	d	a
row 5	w	n	x

Permute rows and columns

	col 1	col 3	col 2
row 3	x	t	a
row 5	w	x	n
row 1	a	t	t
row 4	x	a	d
row 2	a	k	c

- Plaintext: attackxatxdawn
- Ciphertext: xtawxnattxadakc
- Key: matrix size and permutations (3,5,1,4,2) and (1,3,2)

Cryptanalysis: Terminology

- Cryptosystem is **secure** if best known attack is to try all keys
- Cryptosystem is **insecure** if any shortcut attack is known
- By this definition, an insecure system might be harder to break than a secure system! Why?

one-time pad (OTP)

One-Time Pad

A Vigenère cipher with a random key at least as long as the message

- Provably unbreakable
- Why?

Plain text	D O I T	D O N T
Key	A J I Y	A J D Y
Cipher text	D X Q R	D X Q R

- Warning: keys *must* be random, or you can attack the cipher by trying to regenerate the key

Little Bit of History

- about 95 years ago, January 19, 1917 …

Codebook

- Literally, a book filled with "codewords"
- Zimmerman Telegram encrypted via codebook

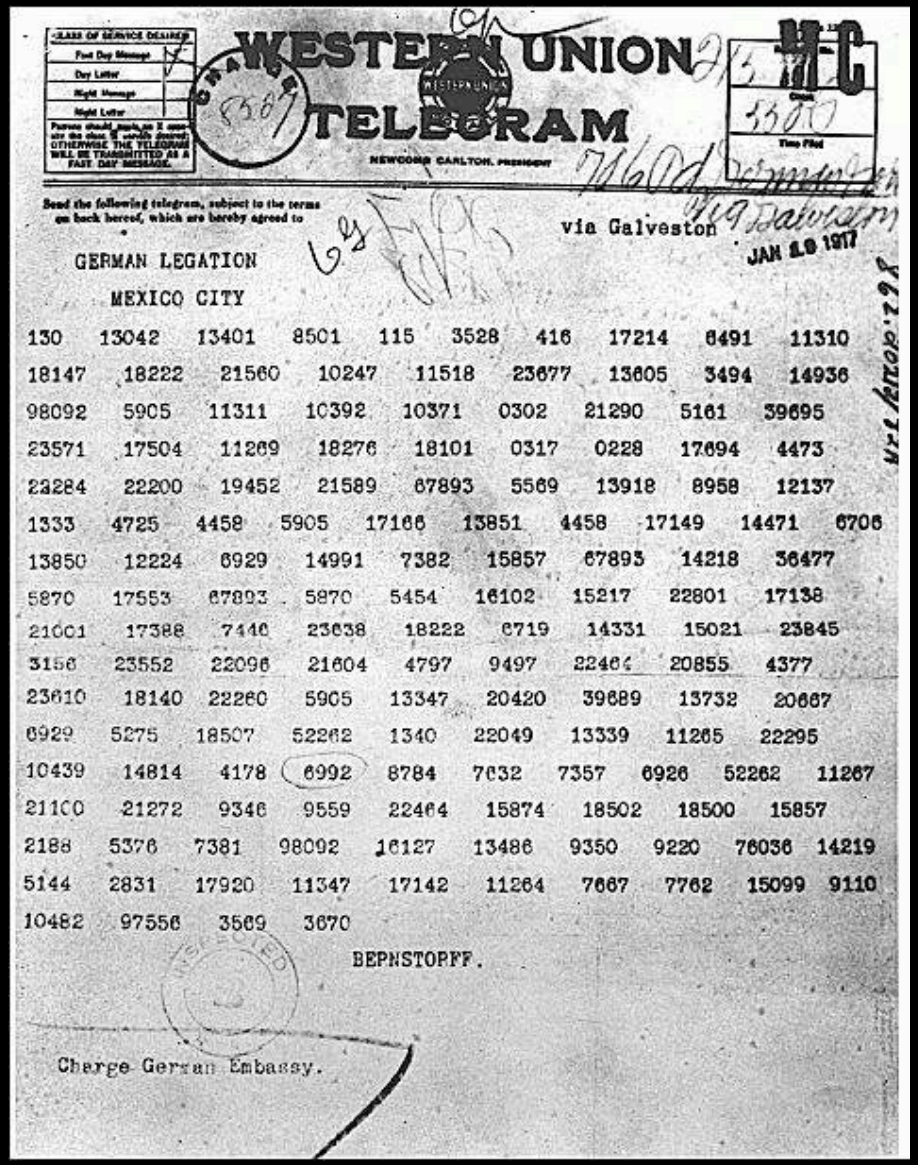
Februar	13605
fest	13732
finanzielle	13850
folgender	13918
Frieden	17142
Friedenschluss	17149
:	:

- Modern block ciphers are codebooks!

Zimmerman Telegram

Arthur Zimmermann (1854-1940)
German Foreign Secretary

- One of most famous codebook ciphers ever
- Led to US entry in WWI
- Ciphertext shown here…



WESTERN UNION TELEGRAM

NEWCOMB CARLTON, PRESIDENT

Send the following telegram, subject to the terms on back hereof, which are hereby agreed to

via Galveston

JAN 19 1917

GERMAN LEGATION
MEXICO CITY

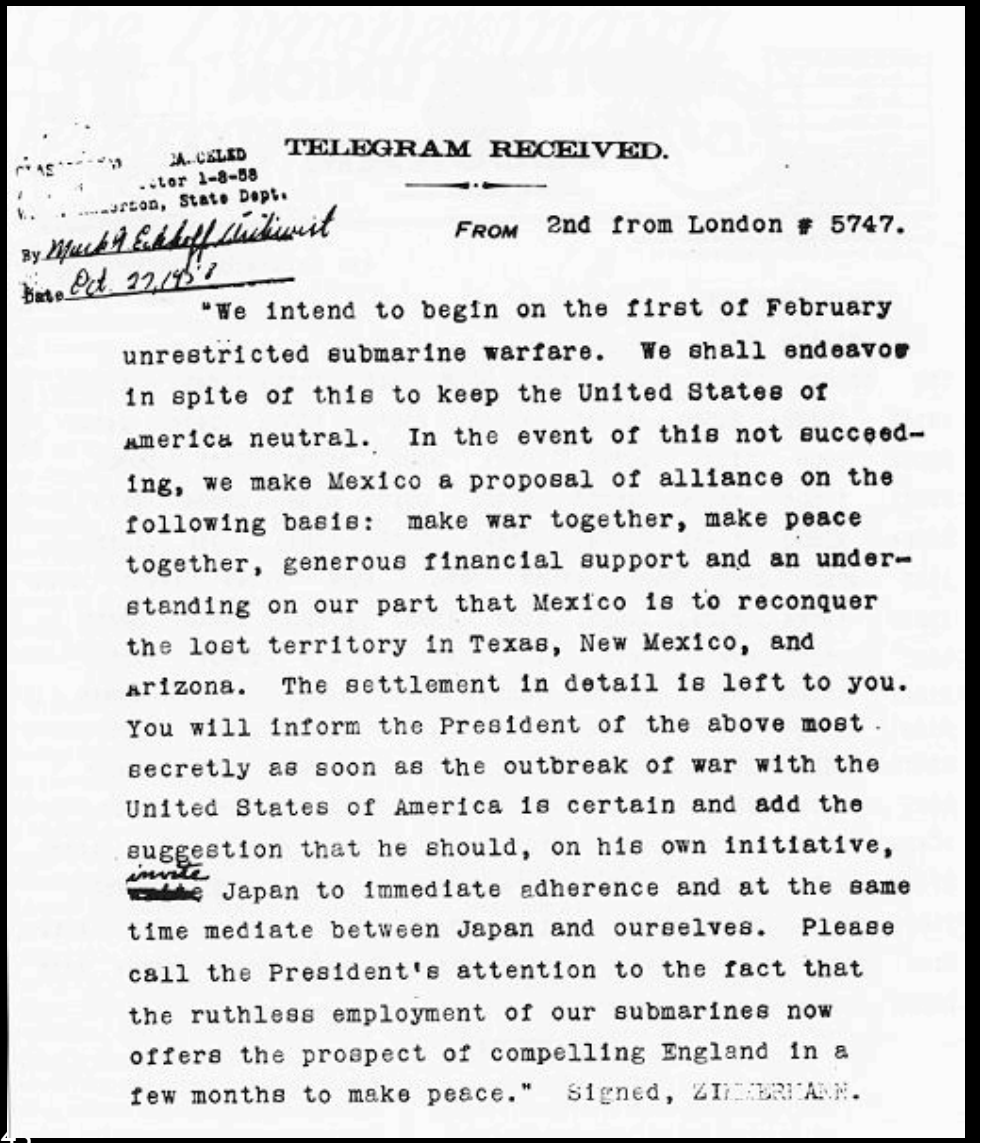
130 13042 13401 8501 115 3528 416 17214 6491 11310
18147 18222 21560 10247 11518 23677 13605 3494 14936
98092 5905 11311 10392 10371 0302 21290 5161 39695
23571 17504 11269 18276 18101 0317 0228 17694 4473
23284 22200 19452 21589 67893 5569 13918 8958 12137
1333 4725 4458 5905 17166 13851 4458 17149 14471 6706
13850 12224 6929 14991 7382 15857 67893 14218 36477
5870 17553 67893 5870 5454 16102 15217 22801 17138
21001 17388 7446 23638 18222 6719 14331 15021 23845
3156 23552 22096 21604 4797 9497 22464 20855 4377
23610 18140 22260 5905 13347 20420 39689 13732 20667
6929 5275 18507 52262 1340 22049 13339 11265 22295
10439 14814 4178 6992 8784 7632 7357 6926 52262 11267
21100 21272 9346 9559 22464 15874 18502 18500 15857
2188 5376 7381 98092 16127 13486 9350 9220 76036 14219
5144 2831 17920 11347 17142 11264 7667 7762 15099 9110
10482 97556 3569 3670

BEPNSTORFF.

Charge German Embassy.

Zimmerman Telegram Decrypted

- British had recovered partial codebook
- Able to fill in missing parts



TELEGRAM RECEIVED.

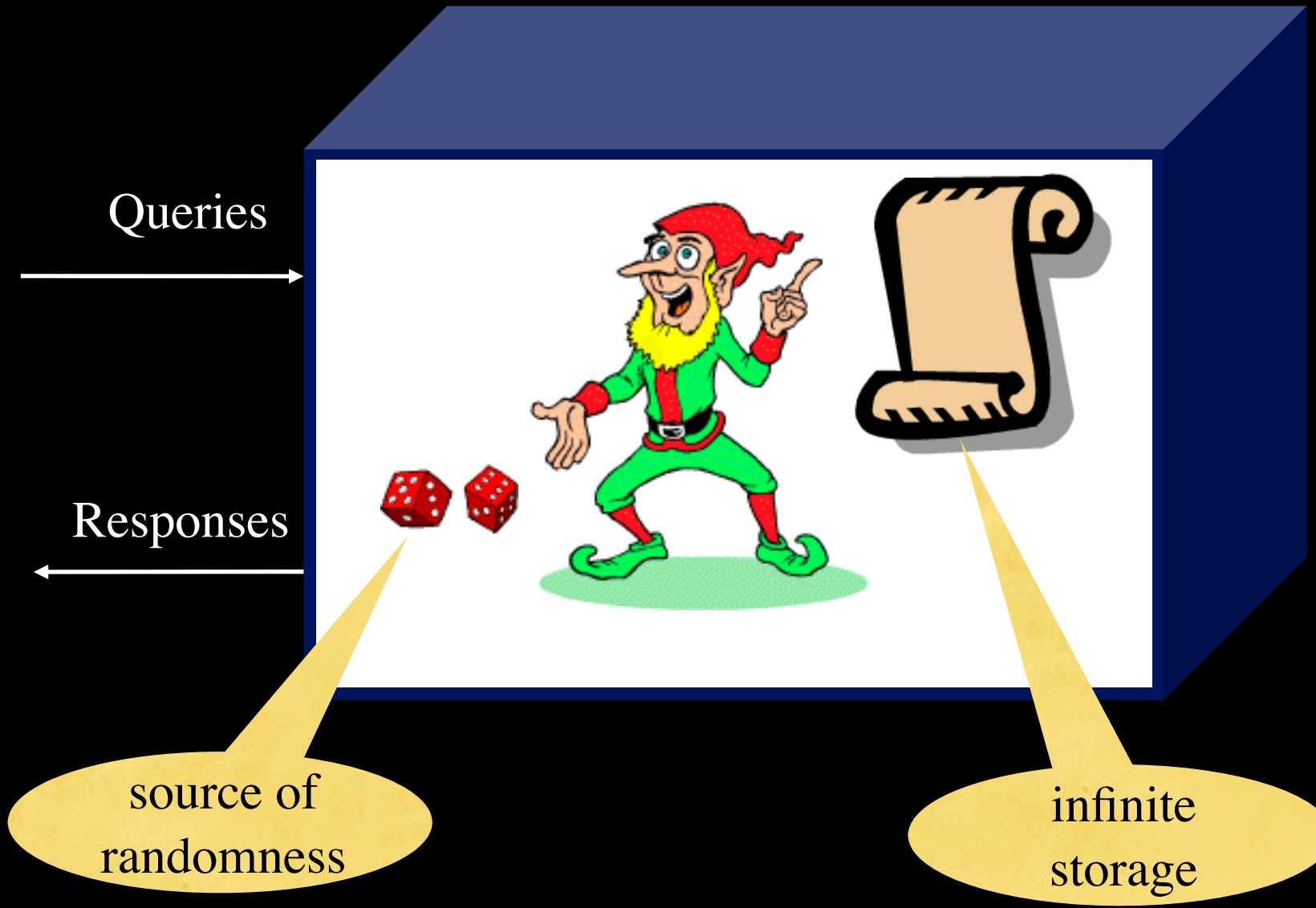
FROM 2nd from London # 5747.

"We intend to begin on the first of February unrestricted submarine warfare. We shall endeavor in spite of this to keep the United States of America neutral. In the event of this not succeeding, we make Mexico a proposal of alliance on the following basis: make war together, make peace together, generous financial support and an understanding on our part that Mexico is to reconquer the lost territory in Texas, New Mexico, and Arizona. The settlement in detail is left to you. You will inform the President of the above most secretly as soon as the outbreak of war with the United States of America is certain and add the suggestion that he should, on his own initiative, invite Japan to immediate adherence and at the same time mediate between Japan and ourselves. Please call the President's attention to the fact that the ruthless employment of our submarines now offers the prospect of compelling England in a few months to make peace." Signed, ZIMMERMANN.

Random Oracle Model

Read Anderson 5.3 from (First Edition)
http://www.cl.cam.ac.uk/~rja14/book.html

What is Random Oracle Model?



Random Function as Random Oracle

- In: string of any length

- Out: random string of fixed length
- Applications:
  - One-way functions
  - Hash functions
    - Message digests
    - Time stamping

Properties

efficiency -- easy to compute h(x) for any x.
one-way -- given any y, it's infeasible to find x, s.t., h(x) = y
weak collision resistance -- given x and h(x), it's infeasible to y != x, s.t. h(y) == h(x)
strong collision resistance -- infeasible to find any x != y, s.t., h(x) == h(y)

Random Generator (Stream Cipher)

as Random Oracle

- In:
  - short string (key)
  - length of the output

- Out: long random stream of bits (keystream)
- Applications:
  - Communications encryption
  - Storage encryption

Properties

- Should not reuse
  - Use *seed*

Example: A5 stream cipher for GSM

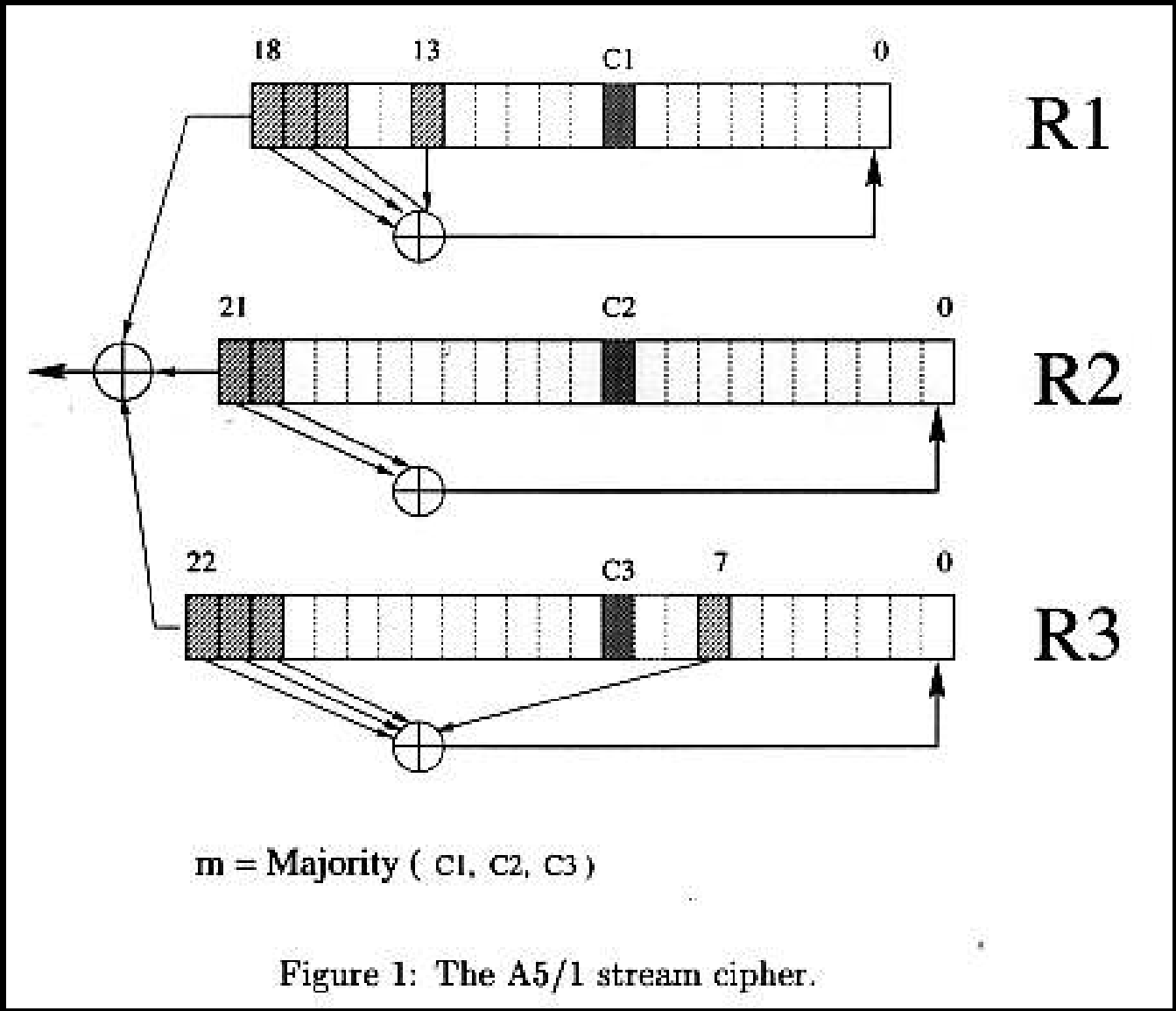
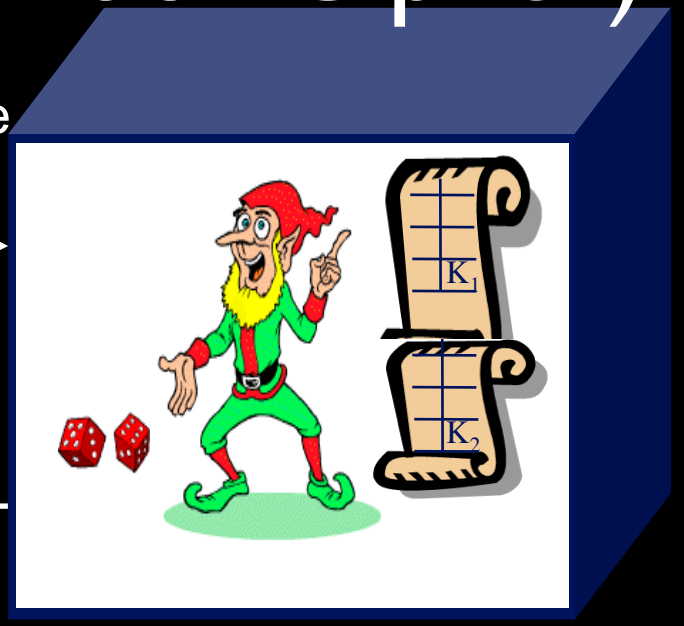


Figure 1: The A5/1 stream cipher.

From: Alex Biryukov, Adi Shamir, David Wagner "Real Time Cryptanalysis of A5/1 on a PC"

Random Permutation (Block Cipher)

as Random Oracle



- In
  - fixed size short string (plaintext) M,
    - DES -- 64 bits
  - Key K
- Out
  - same fixed size short string (ciphertext) C

Notation

- $C = \{ M \}_K$
- $M = \{ C \}_K$

Properties

- Invertible

Summary

- Historical background
  - Caesar, Vigenère, Palyfair, and Double Transpositionciphers
  - One-time pad
  - One-way functions
  - Asymmetric cryptosystems
- The Random Oracle model
  - Random functions: Hash functions
  - Random generators: stream ciphers
  - Random Permutations: block ciphers