THE UNIVERSITY OF BRITISH COLUMBIA

Introduction to Cryptography

EECE 412

Session Outline

- Historical background
  - Caesar and Vigenère ciphers
  - One-time pad
  - One-way functions
  - Asymmetric cryptosystems
- The Random Oracle model
  - Random functions: Hash functions
  - Random generators: stream ciphers
  - Random Permutations: block ciphers
  - Public key encryption and trapdoor one-way permutations
  - Digital signatures

THE UNIVERSITY OF BRITISH COLUMBIA

Historical Background

To read:

5.1-5.2 Anderson’s book

8.1-8.2 Bishop’s book

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
```

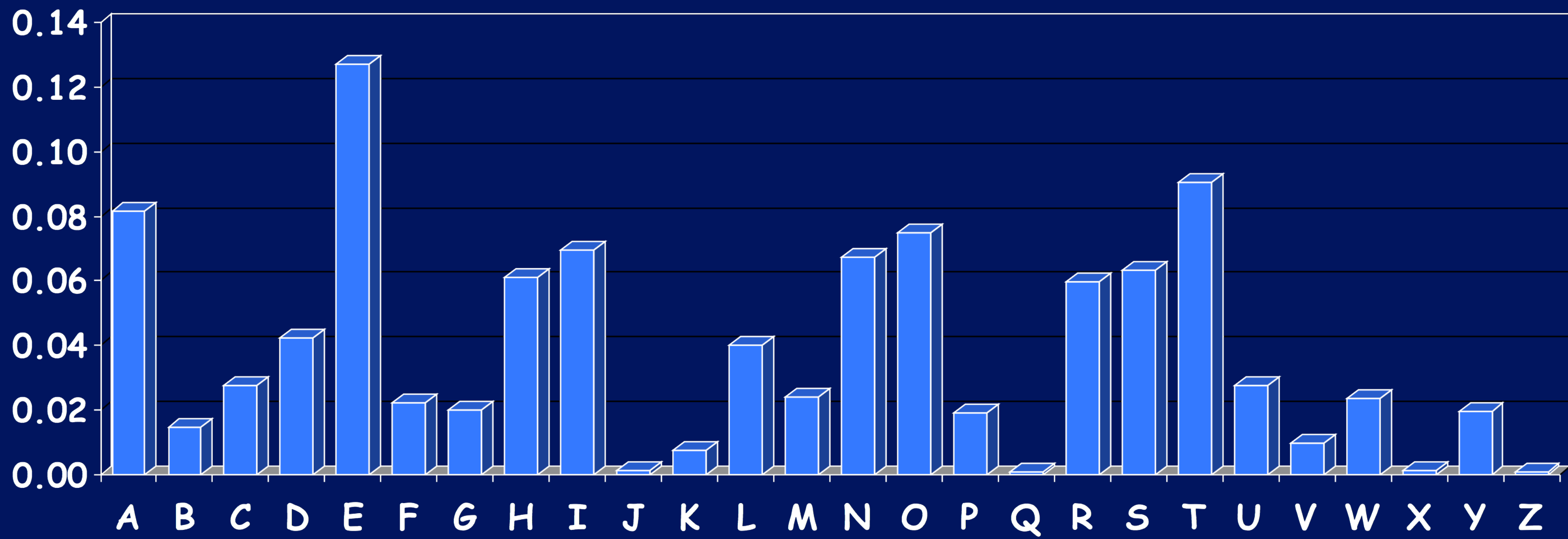
Monoalphabetic Cipher

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



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  IS  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 CSFLZSY
```

Cryptanalysis of Vigenère Cipher

Factoring of distances

- KSMEHZBBLKSMEMPOGAJXSEJCSFLZSY
- 012345678012345678012345678012

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

THE UNIVERSITY OF BRITISH COLUMBIA

Little Bit of History

90 years ago,
January 19, 1917 …

Codebook

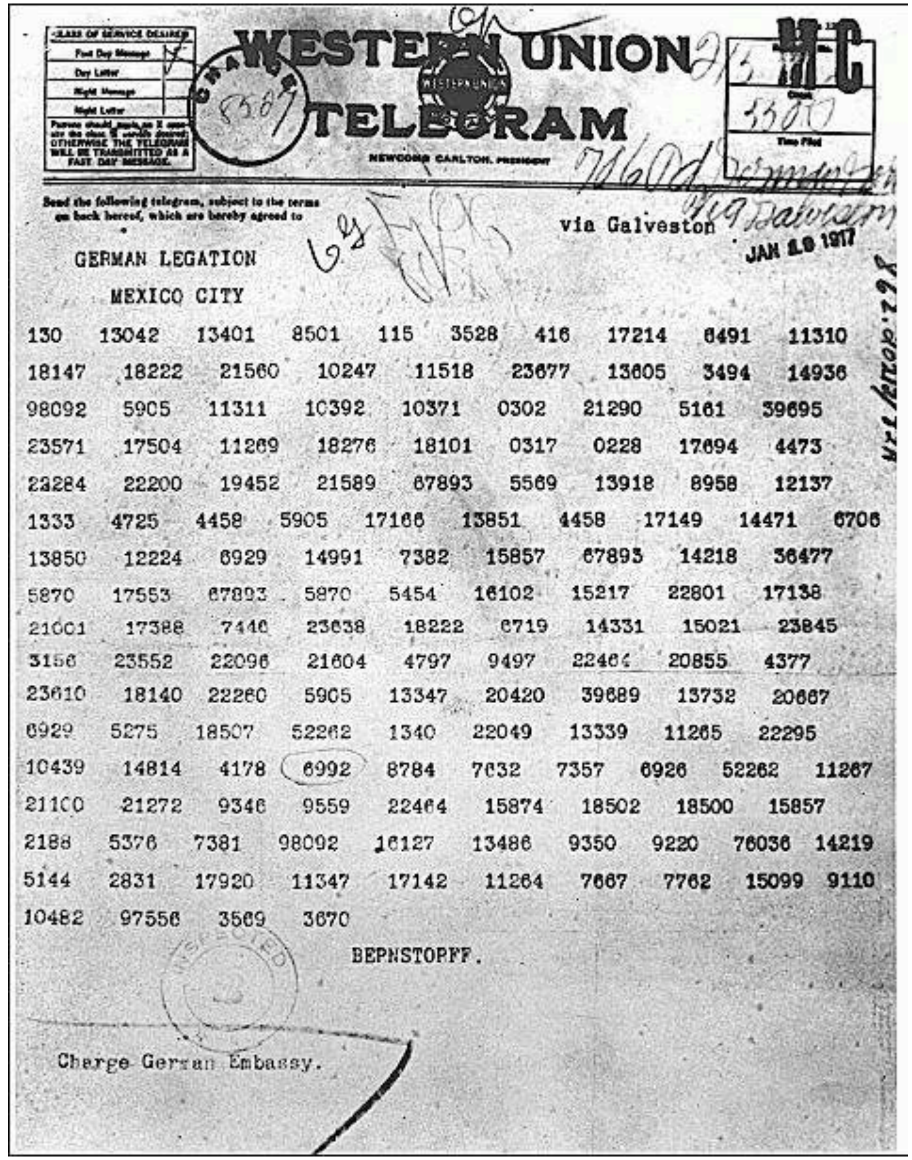
- Literally, a book filled with "codewords"
- Zimmerman Telegram encrypted via codebook

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

- Modern block ciphers are codebooks!

Zimmerman Telegram

- One of most famous codebook ciphers ever
- 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

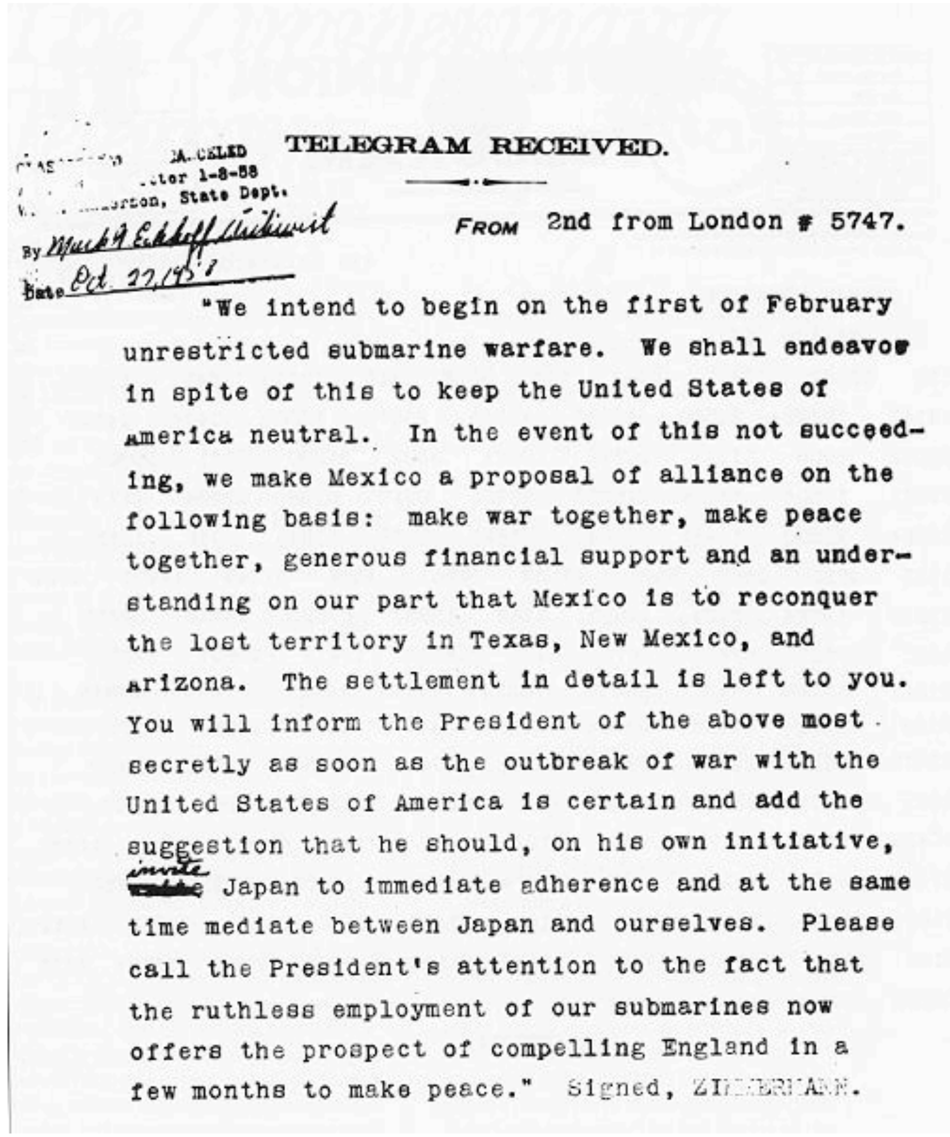
130 13042 13401 8501 115 3528 416 17214 6491 11310
18147 18222 21560 10247 11518 23677 13605 3494 14936
98092 5905 11311 10392 10371 0302 21290 5161 39695
23571 17504 11269 18276 18101 0317 0228 17694 4473
23284 22200 19452 21589 67893 5569 13918 8958 12137
1333 4725 4458 5905 17166 13851 4458 17149 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

BEPNSTOPFF.

Charge German Embassy.

Zimmerman Telegram Decrypted

- British had recovered partial codebook
- Able to fill in missing parts
- Led to US entry in WWI



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.

THE UNIVERSITY OF BRITISH COLUMBIA

Asymmetric Cryptosystems

Public Key Cryptography

- Two keys
  - Sender uses recipient's **public key** to encrypt
  - Receiver uses his **private key** to decrypt
- Based on **trap door, one way function**
  - Easy to compute in one direction
  - Hard to compute in other direction
  - "Trap door" used to create keys
  - Example: Given p and q, product N=pq is easy to compute, but given N, it is hard to find p and q

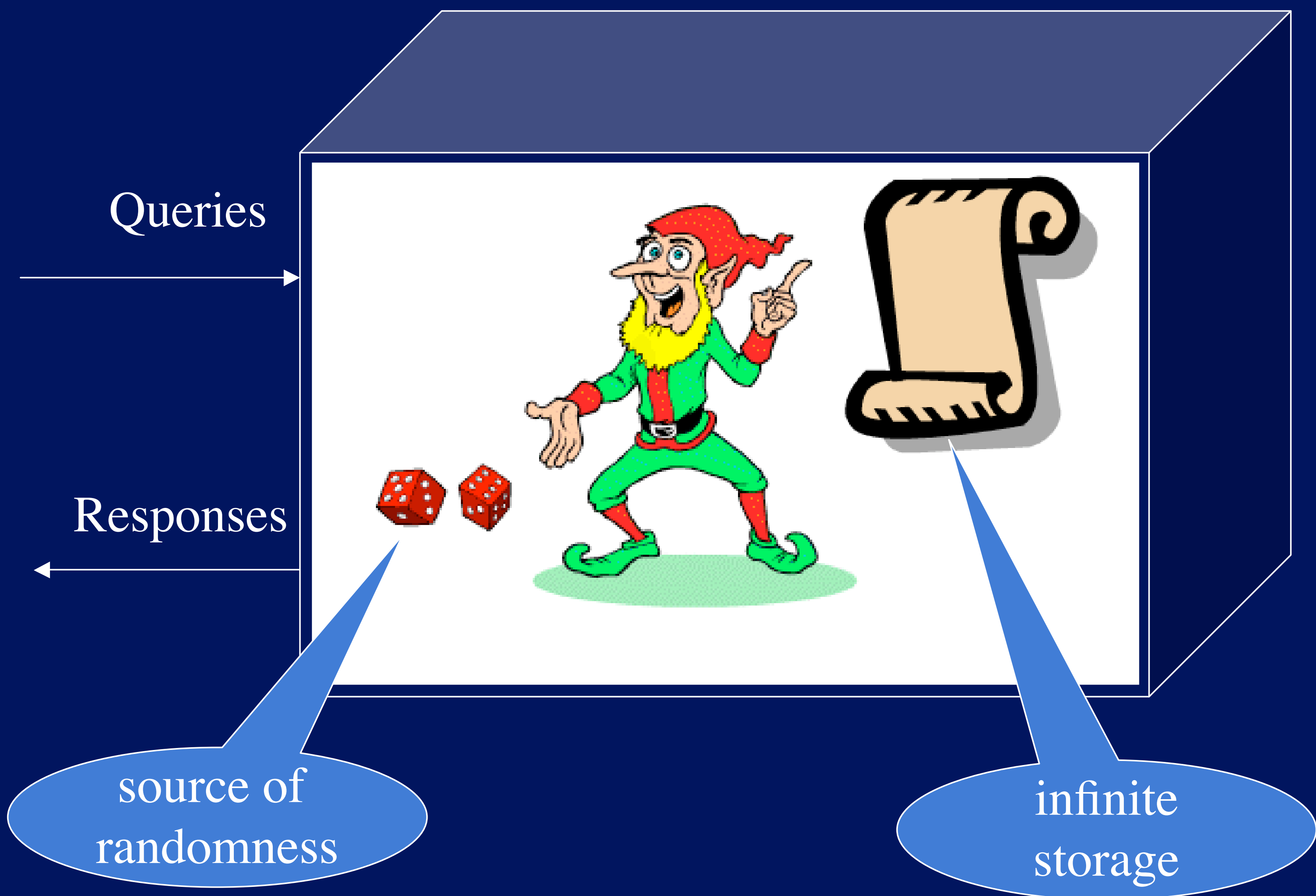
Public Key Cryptography

- Encryption
  - Suppose we encrypt M with Bob's public key
  - Only Bob's private key can decrypt to find M
- Digital Signature
  - **Sign** by "encrypting" with private key
  - Anyone can **verify** signature by "decrypting" with public key
  - But only private key holder could have signed
  - Like a handwritten signature (and then some)

Random Oracle Model

5.3 (Anderson's book)

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

- "One-wayness"
- No input inference from output h(M|K)
- Few collisions

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

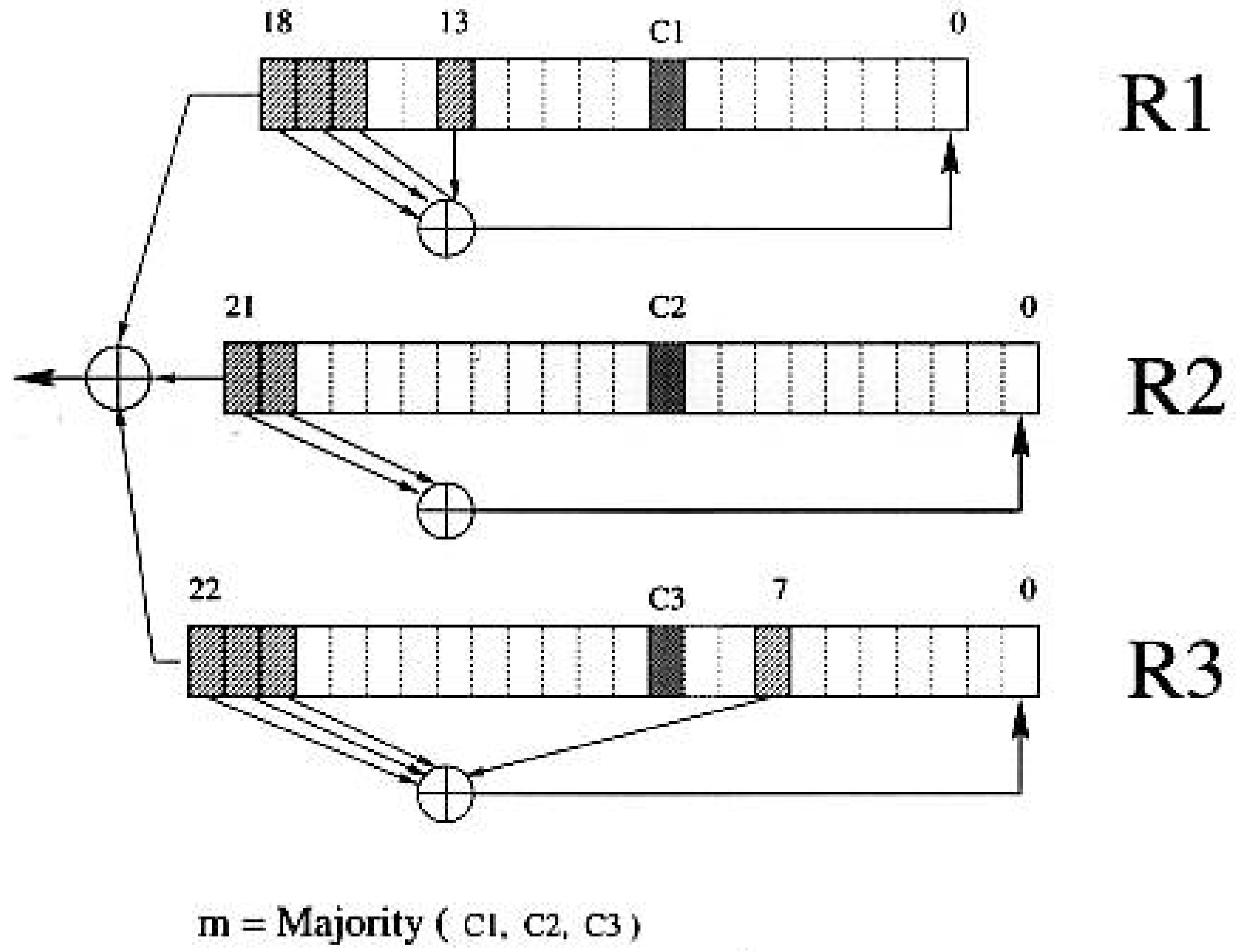


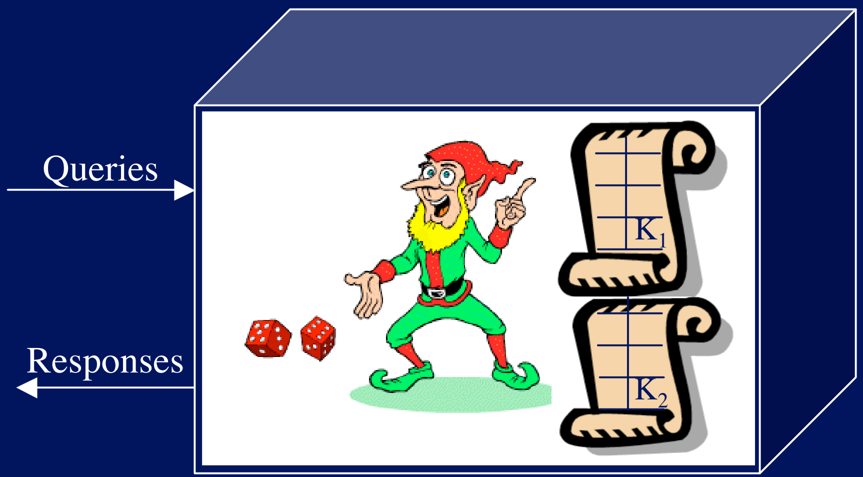
Figure 1: The A5/1 stream cipher.

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

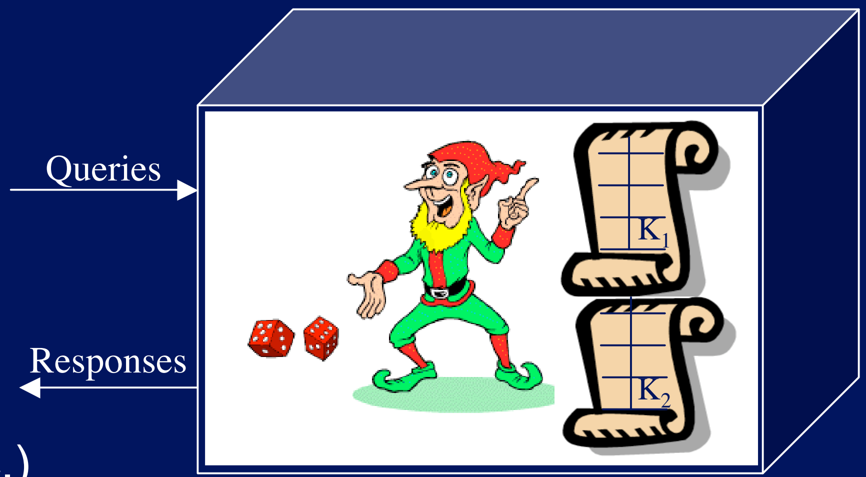
- $C = \{ M \}_K$
- $M = \{ C \}_K$

Properties

- Invertible

Attacks on Block Ciphers

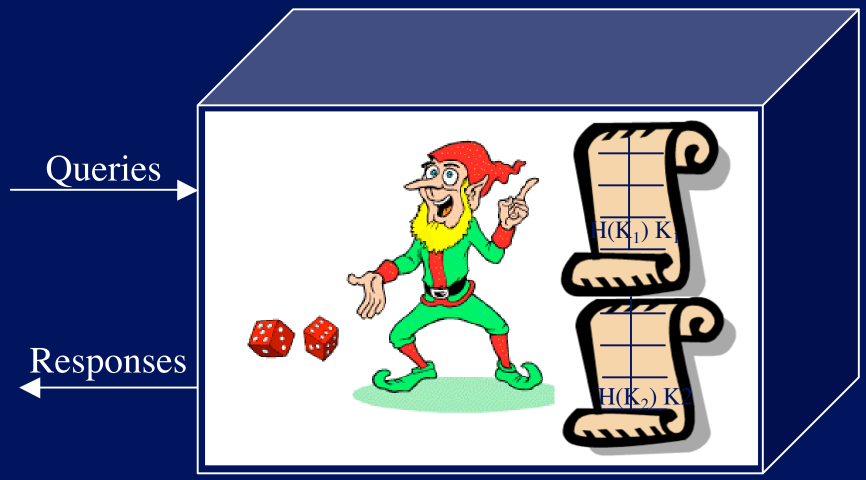
- Attack types
  - Known plaintext attack
  - Chosen plaintext attack
  - Chosen ciphertext attack
  - Chosen plaintext/ciphertext attack
  - Related key attack (K +1, K + 2, etc.)
- Attack objectives
  - forgery attacks-- deduce the answer to the query which the attacker has not made yet
  - key recover attacks -- recover the key
- Why attack types are important?
  - DES
    - 2^{47} chosen plain texts
    - 2^{43} known plain texts



Public Key Encryption and Trap-door One-Way Permutation

as Random Oracle

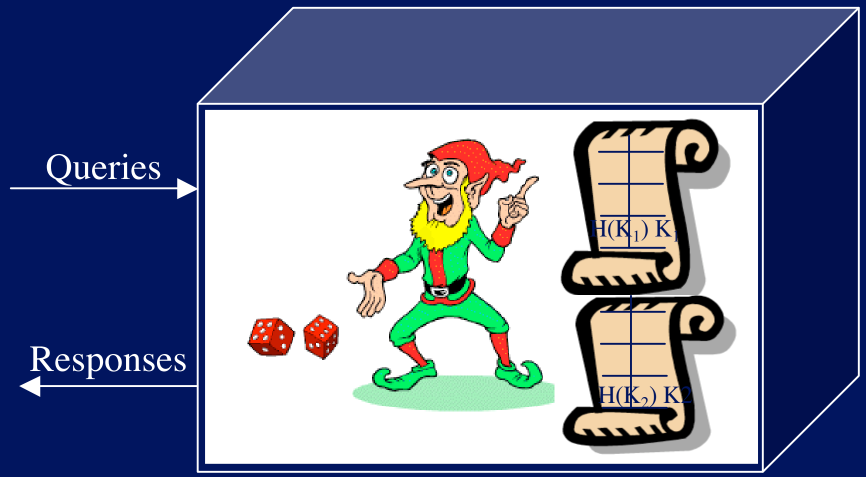
- Public Key Encryption Scheme:
  - Key pair (KR, KR^{-1}) generation function from random string R
    - $KR \rightarrow KR^{-1}$ is infeasible
  - $C = \{M\}_{KR}$
  - $M = \{C\}_{KR^{-1}}$



- In:
  - fixed size short string (plaintext) M,
  - Key KR
- Out: fixed size short string (ciphertext) C

Digital Signature as Random Oracle

- Public Key Signature Scheme:
  - Key pair (σR, VR) generation function
    - VR → σR is infeasible
  - $S = Sig_{\sigma R}(M)$
  - $\{True, False\} = Ver_{VR}(S)$



	Signing	Verifying
Input	Any string M + σR	S + VR
Output	S = hash(M) | cipher block	"True" or "False"

Summary

- Historical background
  - Caesar and Vigenère ciphers
  - One-time pad
  - One-way functions
  - Asymmetric cryptosystems

- The Random Oracle model
  - Random functions: Hash functions
  - Random generators: stream ciphers
  - Random Permutations: block ciphers
  - Public key encryption and trapdoor one-way permutations
  - Digital signatures