

THE UNIVERSITY OF BRITISH COLUMBIA



## Introduction to Cryptography

EECE 412  
Session 3

Copyright © 2004 Konstantin Beznosov

## 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

Copyright © 2004 Konstantin Beznosov

## 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'
  - $C = P + K \text{ mod } 26$
- 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         AGVVEYEVVS  
Cipher     HKGGMAMVGV



### 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 TI ONS RE LA TI ON SR ELA TI ONSREL  
 Cipher KS ME HZ BBL KS ME MPOG AJ XSE J CSFLZSY



7

### Cryptanalysis of Vigenère Cipher

- Factoring of distances
  - KSMEHZBBLKSMEMPOGAJXSEJCSFLZSY
  - 012345678012345678012345678012
- Statistical analysis of each Caesar cipher group
  - KKJZ
  - 1. SSXS
  - 2. MMSY
  - 3. EEE
  - 4. HMJ
  - 5. ZPC
  - 6. BOS
  - 7. BGF
  - 8. LAL



8

### One-Time Pad

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

- Provably unbreakable
- Why?

Plain text	DOIT	DONT
Key	AJIY	AJDY
Cipher text	DXQR	DXQR

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



9

### Asymmetric Cryptosystems

- Public key and private key
  - Encryption
  - Signatures
  - Sep. 21st & 23rd



10

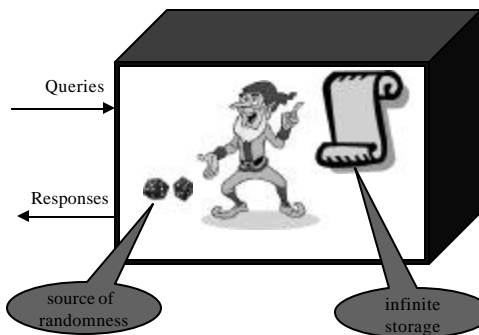


THE UNIVERSITY OF BRITISH COLUMBIA

### Random Oracle Model

Copyright © 2004 Konstantin Beznosov

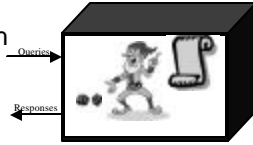
### What is Random Oracle Model?



12

### 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

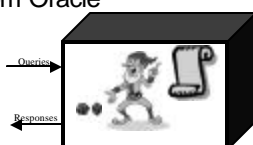
Properties

- "One-wayness"
- No input inference from output
- Few collisions

13

### Random Generator (Stream Cipher) as Random Oracle

- In: short string (key)



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

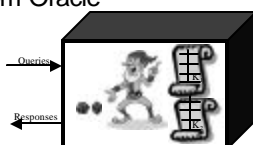
Properties

- Should not reuse
  - Use *seed*

14

### 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

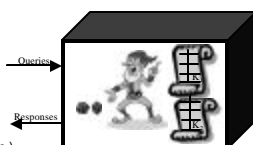
- $C = \{ M \}_K$
- $M = \{ C \}_K$

Properties

- Invertible

15

### Attacks on Block Ciphers

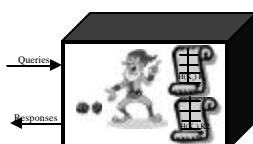


- Attack types
  - Known plaintext attack
  - Chosen plaintext attack
  - Chosen ciphertext attack
  - Chosen plaintext/ciphertext attack
  - Related key attack ( $K + 1, K + 2, \text{etc.}$ )
- Attack objectives
  - Deduce the answer to the query which the attacker has not made yet--forgery attacks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

16

### 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
  - $C = (M)_{KR}$
  - $M = (C)_{KR^{-1}}$

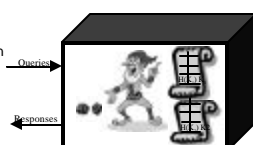


- In:
  - fixed size short string (plaintext)  $M$
  - Key  $KR$
- Out: fixed size short string (ciphertext)  $C$

17

### Digital Signature as Random Oracle

- Public Key Signature Scheme:
  - Key pair ( $\sigma R, VR$ ) generation function
    - $VR \rightarrow \sigma R$  is infeasible
  - $S = \text{Sig}_{\sigma R}(M)$
  - $\{ \text{True}, \text{False} \} = \text{Ver}_{VR}(S)$



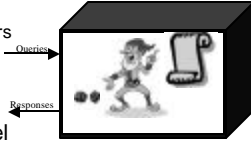
	Signing	Verifying
Input	Any string $M + \sigma R$	$S + VR$
Output	$S = \text{hash}(M) \mid \text{cipher block}$	"True" or "False"

18

## 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

