Cryptography

A Lecture in CE Freshman Seminar Series:
Ten Puzzling Problems in Computer Engineering
About This Presentation

This presentation belongs to the lecture series entitled “Ten Puzzling Problems in Computer Engineering,” devised for a ten-week, one-unit, freshman seminar course by Behrooz Parhami, Professor of Computer Engineering at University of California, Santa Barbara. The material can be used freely in teaching and other educational settings. Unauthorized uses, including any use for financial gain, are prohibited. © Behrooz Parhami

<table>
<thead>
<tr>
<th>Edition</th>
<th>Released</th>
<th>Revised</th>
<th>Revised</th>
<th>Revised</th>
<th>Revised</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Apr. 2012</td>
<td>Apr. 2015</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Puzzles and Cryptograms in Archeology
Secret Codes Are as Old as Forts... and they serve the same purpose providing security!
Some Simple Cryptograms

Cipher: YHPARGOTPYRC OT EMOCLEW
Plain: WELCOME TO CRYPTOGRAPHY

Cipher: EHT YPS WSI RAE GNI LBA CEU TAO
Plain: THE SPY ISW EAR ING ABL UEC OAT

Cipher: ICCRAANCTKBEDLTHIEIVSECYOODEUE

Cipher: SSA PSE TJX SME CRE STO THI GEI
Plain: THI SME SSA GEI STO PSE CRE TJX
Key: 7 4 1 8 6 2 5 3

Cipher: AMY TAN’S TWINS ARE CUTE KIDS
Plain: A T T A C K
Simple Substitution Ciphers

Decipher the following text, which is a quotation from a famous scientist.

**Clue:** Z stands for E

"CEBA YUC YXSENM PDZ SERSESYZ, YXZ QESOZDMZ PEJ XQKPE MYQGSJSYA, PEJ S’K ECY MQDZ PLCQY YXZ RCDKZD."

PBLZDY ZSEMYZSE

"CEBA YUC YXSENM PDZ SERSESYZ, YXZ QESOZDMZ PEJ XQKPE

"**ONLY TWO THINGS ARE INFINITE, THE UNIVERSE AND HUMAN**

MYQGSJSYA, PEJ S’K ECY MQDZ PLCQY YXZ RCDKZD."

**STUPIDITY, AND I’M NOT SURE ABOUT THE FORMER.**"

PBLZDY ZSEMYZSE

X stands for **H**?

ALBERT EINSTEIN

Contextual information facilitated the deciphering of this example

Apr. 2015  
Cryptography  
BParhani
Breaking Substitution Ciphers

The previous puzzle, with punctuation and other give-aways removed:

CEBA YUC YXSENM PDZ SERSESYZ YYZ QESOZDMZ PEJ XQKPE
MYQGSJSYA PEJ SK ECY MQDZ PLCQY YYZ RCDKZD

Letter frequencies in the cipher:

<table>
<thead>
<tr>
<th>Letter</th>
<th>Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td></td>
</tr>
<tr>
<td>B</td>
<td></td>
</tr>
<tr>
<td>C</td>
<td></td>
</tr>
<tr>
<td>D</td>
<td></td>
</tr>
<tr>
<td>E</td>
<td></td>
</tr>
<tr>
<td>F</td>
<td></td>
</tr>
<tr>
<td>G</td>
<td></td>
</tr>
<tr>
<td>H</td>
<td></td>
</tr>
<tr>
<td>I</td>
<td></td>
</tr>
<tr>
<td>J</td>
<td></td>
</tr>
<tr>
<td>K</td>
<td></td>
</tr>
<tr>
<td>L</td>
<td></td>
</tr>
<tr>
<td>M</td>
<td></td>
</tr>
<tr>
<td>N</td>
<td></td>
</tr>
<tr>
<td>O</td>
<td></td>
</tr>
<tr>
<td>P</td>
<td></td>
</tr>
<tr>
<td>Q</td>
<td></td>
</tr>
<tr>
<td>R</td>
<td></td>
</tr>
<tr>
<td>S</td>
<td></td>
</tr>
<tr>
<td>T</td>
<td></td>
</tr>
<tr>
<td>U</td>
<td></td>
</tr>
<tr>
<td>V</td>
<td></td>
</tr>
<tr>
<td>W</td>
<td></td>
</tr>
<tr>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>Z</td>
<td></td>
</tr>
</tbody>
</table>

Letter frequencies in the English language

Most frequently used 3-letter words:
THE AND FOR WAS HIS

Most frequently used letter pairings:
TH HE AN IN ER ON RE ED
The Pigpen Cipher

Encoded message: 

TH H II SS
SS S

This is a substitution cipher, with all the weaknesses of such ciphers.
Run in papers of Friday, Oct. 13, 2006

CELEBRITY CIPHER
by Luis Campos

Celebrity Cipher cryptograms are created from quotations by famous people, past and present. Each letter in the cipher stands for another.

Today's clue: O equals J

"X P Z T F Y B A T H X T R T Y K M Y
M G V Y K X G E J M Z A T Y Y T L Y K M G
G B Y K X G E G B J X W G B J Y K M Y
Z B U T Y X U T Z G B Y K X G E X Z A T Y Y T L."

- E H T G F M O M S W Z B G

PREVIOUS SOLUTION — “Art for the sake of truth, for the sake of what is beautiful and good — that is the creed I seek.” — George Sand

(c) 2006 by NEA, Inc. 10-13
More Sophisticated Substitution Ciphers

The letter A has been replaced by C, D, X, or E in different positions.

The letter T has been replaced by M, W, or X in different positions.

Message

Cipher

25 rotating wheels
The German Enigma Encryption Machine

(1) W pressed on keyboard

(2) Battery now connected to W on plugboard . . .

(3) . . . which is wired to X plug

(4) Connection goes through the 3 rotors, is “reflected”, returns through the 3 rotors, leads to plugboard

(5) Eventually, the “I” light is illuminated

Source: http://www.codesandciphers.org.uk/enigma/index.htm
Alan Turing and the Enigma Project

Alan M. Turing
1912-1954

The German Enigma encryption machine

The Mansion at Bletchley Park
(England’s wartime codebreaking center)

Enigma’s rotor assembly

Source: http://www.ellsbury.com/enigmabombe.htm
More on the Enigma and the Turing Biopic

Brief demo of Enigma (the London Science Museum)
https://youtu.be/TYX691q2J2c

“The Imitation Game” movie trailer
https://www.youtube.com/watch?v=S5CjKEFb-sM

How accurate is “The Imitation Game” biopic?
http://www.slate.com/blogs/browbeat/2014/12/03/the_imitation_game_fact_vs_fiction_how_true_the_new_movie_is_to_alan_turing.html
A Simple Key-Based Cipher

Agreed upon secret key: **ourkey**

Plain text:  
```
ATTACKATDAWN
00 19 19 00 02 10 00 19 03 00 22 13
```

Secret key:  
```
ourkeyourkey
14 20 17 10 04 24 14 20 17 10 04 24
```

Sum:  
```
14 39 36 10 06 34 14 39 20 10 26 37
```

Modulo 26 sum:  
```
14 13 10 10 06 08 14 13 20 10 00 11
```

Cipher text:  
```
ONKKGIONUKAL
```

Secret key:  
```
14 20 17 10 04 24 14 20 17 10 04 24
```

Difference:  
```
00 -7 -7 00 02 -16 00 -7 03 00 -4 -13
```

Modulo 26 diff.:  
```
00 19 19 00 02 10 00 19 03 00 22 13
```

Recovered text:  
```
ATTACKATDAWN
```

One can break such key-based ciphers by doing letter frequency analysis with different periods to determine the key length.

The longer the message, the more successful this method of attack.

---

Apr. 2015  
UCSB  
Cryptography  
BParhami
Decoding a Key-Based Cipher

Agreed upon secret key: **freshman**

Cipher text: `BYELPEYBZIRSTQ`  
```
01 24 04 11 15 04 24 01 25 08 17 18 19 16
```

Secret key: `freshmanfreshman`  
```
05 17 04 18 07 12 00 13 05 17 04 18 07 12
```

Difference: `-4 07 00 -7 08 -8 24-12 20 -9 13 00 12 04`

Modulo 26 diff.: `22 07 00 19 08 18 24 14 20 17 13 00 12 04`

Plain text: `WHATISYOURNAME`

Reply: `JOHNSMITH`  
```
09 14 07 13 18 12 08 19 07
```

Secret key: `freshmanf`  
```
05 17 04 18 07 12 00 13 05
```

Sum: `14 31 11 31 25 24 08 32 12`

Modulo 26 sum: `14 05 11 05 25 24 08 06 12`

Cipher text: `OFLFZYIGM`
Key-Based Cipher with Binary Messages

Agreed upon secret key (11 bits): 0 1 0 0 0 1 1 1 0 1 0

Plain text: 0 0 1 1 1 0 0 1 0 0 1 1 0 0 0
Secret key: 0 1 0 0 0 0 1 1 1 0 1 0 0
XOR: 0 1 1 1 1 1 1 1 0 0 1 1 1 0 0
(mod-2 add)

15 = P
25 = Z
28 = #

Secret key: 0 1 0 0 0 0 1 1 1 0 1 0 0
XOR: 0 0 1 1 1 0 0 1 0 0 1 1 0 0 0

Symmetric: Encoding and decoding algorithms are the same
Data Encryption Standard (DES)

**Feistel block:**
The data path is divided into left \((m_{i-1})\) and right \((m_i)\) halves. A function \(f\) of \(m_i\) and a key \(k_i\) is computed and the result is XORed with \(m_{i-1}\). Right and left halves are then interchanged.

The \(f\) function is fairly complicated, but it has an efficient hardware realization.

**Feistel twisted ladder,**
Preceded and followed by permutation blocks form DES’s encryption, decryption algorithms.
Use of Backdoors in Cryptography

Plaintext \( x \) \( \rightarrow \) Complicated transformation \( f \) \( \rightarrow \) Cipher \( f(x) \)

Inverse function \( f^{-1} \) \( \rightarrow \) \( x \)

Inverse function is a backdoor . . .

Like a hidden latch that releases a magician’s handcuffs
Public-Key Cryptography

Encryption and decryption are asymmetric. Knowledge of the public key does not allow one to decrypt a message.

Electronic signature (authentication)


E.g., key for symmetric communication
Alice sends a secret message to Bob by putting the message in a box and using one of Bob’s padlocks to secure it. Only Bob, who has a key to his padlocks, can open the box to read the message.
RSA Public Key Algorithm

Choose large primes $p$ and $q$
Compute $n = pq$
Compute $m = (p - 1)(q - 1)$
Choose small $e$ coprime to $m$
Find $d$ such that $de = 1 \mod m$
Publish $n$ and $e$ as public key
Keep $n$ and $d$ as private key

$p = 7, q = 19$
$n = 7 \times 19 = 133$
$m = 6 \times 18 = 108$
e = 5
d = 65
Public key: 133, 5
Private key: 133, 65

Security of RSA is due to the difficulty of factoring large numbers
Therefore, $p$ and $q$ must be very large: 100s of bits

Encryption example:

$$y = x^e \mod n$$

$$= 6^5 \mod 133$$

$$= 7776 \mod 133$$

$$= 62$$

Decryption example:

$$x = y^d \mod n$$

$$= 62^{65} \mod 133$$

$$= 62(3844)^{32} \mod 133$$

$$= 62(120)^{32} \mod 133 = \ldots = 6$$