

Principles of Information Security CS 5323 Lecture Ten

Prof. William Winsborough
October 21, 2008

Business

- I will return the exams this Thursday
- This week is about chapter 8
- Next week we will start chapter 9 (reading)
- Questions from previous lectures?

21 October 2008

Winsborough CS 5323 Lecture 10

2

Vigènere Cipher

- Like Cæsar cipher, but use a phrase
- Example
 - Message THE BOY HAS THE BALL
 - Key VIG
 - Encipher using Cæsar cipher for each letter:
key VIGVIGVIGVIGVIGV
plain THEBOYHASTHEBALL
cipher OPKWECIYOPKWIRG

21 October 2008

Winsborough CS 5323 Lecture 10

3

Relevant Parts of Tableau

	<i>G</i>	<i>I</i>	<i>V</i>
<i>A</i>	G	I	V
<i>B</i>	H	J	W
<i>E</i>	L	M	Z
<i>H</i>	N	P	C
<i>L</i>	R	T	G
<i>O</i>	U	W	J
<i>S</i>	Y	A	N
<i>T</i>	Z	B	O
<i>Y</i>	E	H	T

- Tableau shown has relevant rows, columns only
- Example encipherments:
 - key V, letter T: follow V column down to T row (giving "O")
 - Key I, letter H: follow I column down to H row (giving "P")

21 October 2008

Winsborough CS 5323 Lecture 10

4

Useful Terms

- *period*: length of key
 - In earlier example, period is 3
- *tableau*: table used to encipher and decipher
 - Vigènere cipher has key letters on top, plaintext letters on the left
- *polyalphabetic*: the key has several different letters
 - Cæsar cipher is monoalphabetic

21 October 2008

Winsborough CS 5323 Lecture 10

5

Attacking the Cipher

- Approach
 - Establish period; call it n
 - Break message into n parts, each part being enciphered using the same key letter
 - Solve each part
 - You can leverage one part from another
- We will show each step

21 October 2008

Winsborough CS 5323 Lecture 10

6

The Target Cipher

- We want to break this cipher:

```
ADQYS MIUSB OXKKT MIBHK IZOOO
EQOOG IFBAG KAUMF VVTAA CIDTW
MOCIO EQOOG BMBFV ZGGWP CIEKQ
HSNEW VECNE DLA AV RWKXS VNSVP
HCEUT QOIOF MEGJS WTPCH AJMOC
HIUIX
```

Establish Period

- Kasiski:** repetitions in the ciphertext occur when characters of the key appear over the same characters in the plaintext
- Example:

```
key      VIGVIGVIGVIGVIGV
plain    THEBOYHASTHEBALL
cipher   OPKWWECIYOPKWIRG
```

Note the key and plaintext line up over the repetitions (underlined). As distance between repetitions is 9, the period is a factor of 9 (that is, 1, 3, or 9)

Repetitions in Example

Letters	Start	End	Distance	Factors
MI	5	15	10	2, 5
OO	22	27	5	5
OEQOOG	24	54	30	2, 3, 5
FV	39	63	24	2, 2, 2, 3
AA	43	87	44	2, 2, 11
MOC	50	122	72	2, 2, 2, 3, 3
QO	56	105	49	7, 7
PC	69	117	48	2, 2, 2, 2, 3
NE	77	83	6	2, 3
SV	94	97	3	3
CH	118	124	6	2, 3

Estimate of Period

- OEQOOG is probably not a coincidence
 - It's too long for that
 - Period may be 1, 2, 3, 5, 6, 10, 15, or 30
- Most others (7/10) have 2 in their factors
- Almost as many (6/10) have 3 in their factors
- Begin with period of $2 \times 3 = 6$

Check on Period

- Index of coincidence is probability that two randomly chosen letters from ciphertext will be the same
- Tabulated for different periods:

1	0.066	3	0.047	5	0.044
2	0.052	4	0.045	10	0.041
Large	0.038				

Compute IC

- $IC = [n(n-1)]^{-1} \sum_{0 \leq i \leq 25} [F_i(F_i-1)]$
 - where n is length of ciphertext and F_i the number of times character i occurs in ciphertext
- Here, $IC = 0.043$
 - Indicates a key of slightly more than 5
 - A statistical measure, so it can be in error, but it agrees with the previous estimate (which was 6)

Splitting Into Alphabets

alphabet 1: AIKHOIATTOBGEEERNEOSAI

alphabet 2: DUKKEFUAWEMGKWDWSUFWJU

alphabet 3: QSTIQBMAMQBWQVLKVTMTMI

alphabet 4: YBMZOAFCOOPHEAXPQEPOX

alphabet 5: SOIOOGVICOVCSVASHOGCC

alphabet 6: MXBOGKVDIGZINNVVCIJHH

- ICs (#1, 0.069; #2, 0.078; #3, 0.078; #4, 0.056; #5, 0.124; #6, 0.043) indicate all alphabets have period 1, except #4 and #6; assume statistics off

21 October 2008

Winsborough CS 5323 Lecture 10

13

Frequency Examination

ABCDEFGHIJKLMNOPQRSTUVWXYZ

1 31004011301001300112000000

2 10022210013010000010404000

3 12000000201140004013021000

4 21102201000010431000000211

5 10500021200000500030020000

6 01110022311012100000030101

Letter frequencies are (H high, M medium, L low):

HMMMHHMMHHMMHHMLHHHMLLLLLL

21 October 2008

Winsborough CS 5323 Lecture 10

14

Begin Decryption

- First matches characteristics of unshifted alphabet
- Third matches if I shifted to A
- Sixth matches if V shifted to A
- Substitute into ciphertext (bold are substitutions)

ADIYS RIUKB OCKKL MIGHK AZOTO EIOOL
 IFTAG PAUEF VATAS CIITW **EOCNO** EIOOL
 BMTFV **EGGOP** CNEKI HSSEW **NECSE** DDAAA
 RWXCS **ANSNP** HHEUL QONOF **EEGOS** WLPCM
AJEOC MIUAX

21 October 2008

Winsborough CS 5323 Lecture 10

15

Look For Clues

- **AJE** in last line suggests "are", meaning second alphabet maps A into S:

ALIYS RICKB OCKSL MIGHS AZOTO
 MIOOL INTAG **PACEF** VATIS CIITE
 EOCNO MIOOL BUTFV EGOOP CNESI
 HSSEE **NECSE** LDAAA **RECX**S ANANP
 HHECL QONON EEGOS ELPCM AREOC
MICAX

21 October 2008

Winsborough CS 5323 Lecture 10

16

Next Alphabet

- **MICAX** in last line suggests "mical" (a common ending for an adjective), meaning fourth alphabet maps O into A:

ALIMS RICKP OCKSL AIGHS ANOTO MICOL
 INTOG PACET VATIS **QIITE** ECCNO MICOL
 BUTTV EGOOD CNESI VSSEE NSCSE LDOAA
 RECLS ANAND HHECL EONON ESGOS ELDCM
ARECC MICAL

21 October 2008

Winsborough CS 5323 Lecture 10

17

Got It!

- **QI** means that U maps into I, as Q is always followed by U:

ALIME RICKP ACKSL AUGHS ANATO MICAL
 INTOS PACET HATIS **QUITE** ECONO MICAL
 BUTTH EGOOD ONESI VESEE NSOSE LDOMA
 RECLE ANAND THECL EANON ESSOS ELDOM
ARECO MICAL

21 October 2008

Winsborough CS 5323 Lecture 10

18

One-Time Pad

- A Vigenère cipher with a random key at least as long as the message
 - Provably unbreakable
 - Why? Look at ciphertext $DXQR$. Equally likely to correspond to plaintext $DOIT$ (key $AJYI$) and to plaintext $DONT$ (key $AJDY$) and any other 4 letters
 - Warning: keys *must* be random, or you can attack the cipher by trying to regenerate the key
 - Approximations, such as using pseudorandom number generators to generate keys, are *not* random

21 October 2008

Winsborough CS 5323 Lecture 10

19

Overview of the DES

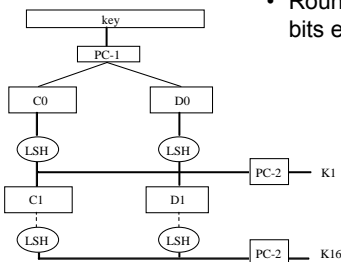
- A block cipher:
 - encrypts blocks of 64 bits using a 64 bit key
 - outputs 64 bits of ciphertext
- A product cipher
 - basic unit is the bit
 - performs both substitution and transposition (permutation) on the bits
- Cipher consists of 16 rounds (iterations) each with a round key generated from the user-supplied key

21 October 2008

Winsborough CS 5323 Lecture 10

20

Generation of Round Keys



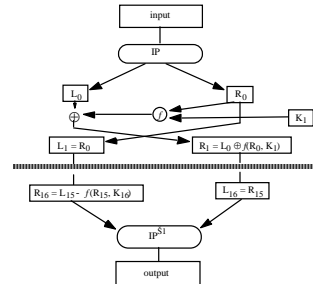
- Round keys are 48 bits each

21 October 2008

Winsborough CS 5323 Lecture 10

21

Encipherment

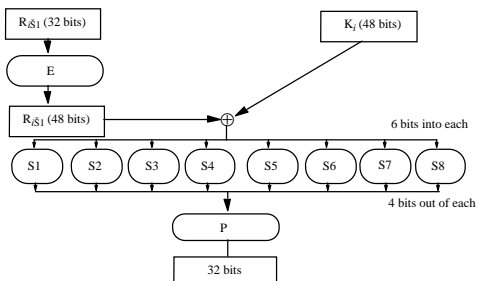


21 October 2008

Winsborough CS 5323 Lecture 10

22

The f Function



21 October 2008

Winsborough CS 5323 Lecture 10

23

Controversy

- Considered too weak
 - Diffie, Hellman said in a few years technology would allow DES to be broken in days
 - Design using 1999 technology published
 - Design decisions not public
 - S-boxes may have backdoors

21 October 2008

Winsborough CS 5323 Lecture 10

24

Undesirable Properties

- 4 weak keys
 - They are their own inverses
- 12 semi-weak keys
 - Each has another semi-weak key as inverse
- Complementation property
 - $DES_k(m) = c \Rightarrow DES_k(m') = c'$
- S-boxes exhibit irregular properties
 - Distribution of odd, even numbers non-random
 - Outputs of fourth box depends on input to third box

21 October 2008

Winsborough CS 5323 Lecture 10

25

Differential Cryptanalysis

- A chosen ciphertext attack
 - Requires 2^{47} plaintext, ciphertext pairs
- Revealed several properties
 - Small changes in S-boxes reduce the number of pairs needed
 - Making every bit of the round keys independent does not impede attack
- Linear cryptanalysis improves result
 - Requires 2^{43} plaintext, ciphertext pairs

21 October 2008

Winsborough CS 5323 Lecture 10

26

DES Modes

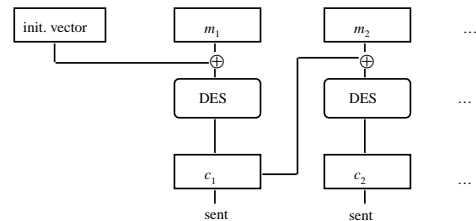
- Electronic Code Book Mode (ECB)
 - Encipher each block independently
- Cipher Block Chaining Mode (CBC)
 - Xor each block with previous ciphertext block
 - Requires an initialization vector for the first one
- Encrypt-Decrypt-Encrypt Mode (2 keys: k, k')
 - $c = DES_k(DES_{k'}^{-1}(DES_k(m)))$
- Encrypt-Encrypt-Encrypt Mode (3 keys: k, k', k'')
 - $c = DES_k(DES_{k'}(DES_{k''}(m)))$

21 October 2008

Winsborough CS 5323 Lecture 10

27

CBC Mode Encryption

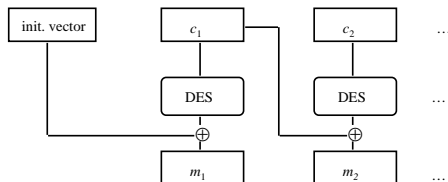


21 October 2008

Winsborough CS 5323 Lecture 10

28

CBC Mode Decryption



21 October 2008

Winsborough CS 5323 Lecture 10

29

Self-Healing Property

- Initial message
 - 3231343336353837 3231343336353837
3231343336353837 3231343336353837
- Received as (underlined 4c should be 4b)
 - ef7c4cb2b4ce6f3b f6266e3a97af0e2c
746ab9a6308f4256 33e60b451b09603d
- Which decrypts to
 - efca61e19f4836f1 3231333336353837
3231343336353837 3231343336353837
 - Incorrect bytes underlined
 - Plaintext “heals” after 2 blocks

21 October 2008

Winsborough CS 5323 Lecture 10

30

Current Status of DES

- Design for computer system, associated software that could break any DES-enciphered message in a few days published in 1998
- Several challenges to break DES messages solved using distributed computing
- NIST selected Rijndael as Advanced Encryption Standard, successor to DES
 - Designed to withstand attacks that were successful on DES