CENG 520 –Lecture Note II

NUMERAL CODING

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

Classical Ciphers(Paper-pencil Systems)

Two types:

- Substitution Ciphers : the units of the plaintext are retained in the same sequence in the ciphertext, but the units themselves are altered
- Transposition Ciphers : the ciphertext constitutes a permutation of the plaintext

http://www.murky.org/cryptography/classical.shtml

Shift Cipher-Ceasar Shift

Ciphertext alphabet is obtained from the plaintext alphabet by a shift transformation $E_k(p)=p+k \bmod 26$ with the key k.

PLAINTEXT	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**	**j**	**k**	**l**	**m**
CIPHERTEXT	D	E	F	G	H	I	J	K	L	M	N	O	P
PLAINTEXT	n	o	p	q	r	s	t	u	v	w	x	y	z
CIPHERTEXT	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

hello there → KHOORWKHUH

Encryption function: $E_k(x) = (x + k) \bmod 26$
Decryption function: $D_k(x) = (x - k) \bmod 26$

Problem

- Monoalphabetic -- Same letter of plaintext always produces same letter of ciphertext
- Even though there are 26! possible substitutions, monoalphabetic solutions are easy to break!
- Use frequency analysis of English language, plus some tricks...

Example

Ciphertext : HFSPFDF Key:? Plaintext:?

Clue: Plaintext is Turkish (Plaintext alphabet: English)

Answer: Key :5 Plaintext: CANKAYA

Frequencies of the letters of the English alphabet:

High	%	Middle	%	Low	%
E	12.31	L	4.03	B	1.62
T	9.59	D	3.65	G	1.61
A	8.05	C	3.20	V	.93
O	7.94	U	3.10	K	.52
N	7.19	P	2.29	Q	.20
I	7.18	F	2.28	X	.20
S	6.59	M	2.25	J	.10
R	6.03	W	2.03	Z	.09
H	5.14	Y	1.88		

The most frequent letters in some languages:

ENGLISH		GERMAN		FINNISH		FRENCH		ITALIAN		SPANISH	
	%		%		%		%		%		%
E	12.31	E	18.46	A	12.06	E	15.87	E	11.79	E	13.15
T	9.59	N	11.42	I	10.59	A	9.42	A	11.74	A	12.69
A	8.05	I	8.02	T	9.76	I	8.41	I	11.28	O	9.49
O	7.94	R	7.14	N	8.64	S	7.90	O	9.83	S	7.60
N	7.19	S	7.04	E	8.11	T	7.26	N	6.88	N	6.95
I	7.18	A	5.38	S	7.83	N	7.15	L	6.51	R	6.25

Breaking a Monoalphabetic Substitution

Yxdy pq yjc xzpvpyw ya icqdepzc ayjceq xq
Tact is the ability to describe others as
yjcw qcc yjcuqcvrcq.
they see themselves.

Xzexjxu Vpsdavs
Abraham Lincoln

Character Frequency: C10, Y8, Q7, X6, J5, P5, V4, D3, A3, E3, Z3, S2, U 2, I1, R1, W2

Alphabet frequency: e t a o i n s r h l d c u m f p g w y b v k x j q z

Monoalphabetic/Polyalphabetic

Substitution ciphers can be classified as being monoalphatic or polyalphabetic and monographic or polygraphic.

- Monoalphabetic: each possible symbol is given a unique replacement symbol
- Polyalphabetic: encrypts a two or more letters at each step

SHIFT TRANSFORMATION (DIGRAPHIC)

- Blocksize=2, calculations in Z/676Z
- $E_k(x)=x+k$
- Example: k=347

Plain text in pairs	A B	E T	T E	R B ...
Encoding	0001	0419	1904	1701 ...
26x+y	1	123	498	443 ...
Shifting(+347)	348	470	164	114 ...
Expressing in base 26	1310	1802	0613	0410...
Decoding	N K	S C	G N	E K...
Ciphertext	NKSCG NEK...			

Most frequent digrams in English

	%		%		%
TH	6.3	AR	2.0	HA	1.7
IN	3.1	EN	2.0	OU	1.4
ER	2.7	TI	2.0	IT	1.4
RE	2.5	TE	1.9	ES	1.4
AN	2.2	AT	1.8	ST	1.4
HE	2.2	ON	1.7	OR	1.4

Homework

- **SHIFT CIPHER (HEXAGRAPGHIC: BLOCKSIZE=6)**
- KEY : 178455741 (k)
- Plaintext:
  SINCETIMECANBEMEASUREDWITHEXTREMEPRECISI
  ONANDSINCECISALSOKNOWNWITHGREATPRECISION
  THISRESULTSINANEXTREMELYACCURATEMEASUREM
  ENTOFTHEDISTANCEBETWEENTHERADARANTENNA
  WHICHLAUNCHESTHEPULSEANDTHENEARESTPOINT
  ONTHEPLANETWHICHREFLECTSITUNFORTUNATELYT
  HESTRENGTHOFTHERETURNINGECHODROPSOFFWIT
  HTHEFOURTHPOWEROFDISTANCEANDSOTHISVERYAC
  CURATETECHNIQUEISLIMITEDTOTHESOLARSYSTEMB
  UTITSEMPLOYMENTDOESMEANTHATALLSOLARSYSTE
  MDISTANCESAREKNOWNWITHGREATPRECISION

Affine Cipher

- Encryption function: $E_{a,b}(x) = (ax + b) \bmod 26$
- Decryption function: $D_{a,b}(x) = (a^{-1}x – a^{-1}b) \bmod 26$

where the pair (a,b) is the key.

- To have an invertible transformation one must have gcd(a,26)=1.

Example:

Key: (7,12)
PLAIN ALPHABET: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
CIPHER ALPHABET: M T A H O V C J Q X E L S Z G N U B I P W D K R Y F

Simple Substitution (Monoalphabetic)

- First, the letters of the keyword is written without repetitions, then the unused letters of the alphabet are written in their usual ordering.

Example:

Key: LOVEBIRD
PLAIN ALPHABET: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
CIPHER ALPHABET: L O V E B I R D A C F G H J K M N P Q S T U W X Y Z

Vigenere Cipher (Repetitive Key)

- The keyword is written repeatedly below the plaintext and corresponding letters are added modulo 26.

Key: LOVEBIRD								
Plaintext:	BIRDS	LOVEW	HEATB	READB	ROWNR	ICEAN	DAWON	DERFU
Key :	LOVEB	IRDLO	VEBIR	DLOVE	BIRDL	OVEBI	RDLOV	EBIRD
Ciphertext:	MWMHT	TFYPK	CIBBS	UPOYF	SWNQC	WXIBV	UDHCI	HFZWX

Vigenere Cipher (Progressive Key)

- Same as the Vigenere repetitive key cipher with only difference, the letters of the key is shifted by 1 at each repetition

Key: LOVEBIRD								
Plaintext:	BIRDS	LOVEW	HEATB	READB	ROWNR	ICEAN	DAWON	DERFU
Key :	LOVEB	IRDMP	WFCJS	ENQXG	DKTFO	RYHEL	UGPSZ	IFMVH
Ciphertext:	MWMHT	TFYQL	DJCCT	VRQAH	UYPSF	ZALEY	XGLGM	LJDAB

Vigenere Cipher (Autoclave)

- Same as the Vigenere repetitive key cipher with only difference, the key is used only once then it is followed by the plaintext.

Key: LOVEBIRD								
Plaintext:	BIRDS	LOVEW	HEATB	READB	ROWNR	ICEAN	DAWON	DERFU
Key :	LOVEB	IRDBI	RDSLO	VEWHE	ATBRE	ADBRO	WNRIC	EANDA
Ciphertext:	MWMHT	TFYFE	YHSEP	MIWKF	RHXEV	IFFRB	ZNNWP	HEEIU

Vigenere Cipher (Key+Ciphertext)

- Same as the autoclave mode but the key is followed by the ciphertext

Key: LOVEBIRD								
Plaintext:	BIRDS	LOVEW	HEATB	READB	ROWNR	ICEAN	DAWON	DERFU
Key :	LOVEB	IRDMW	MHTTF	YQSTL	TMGPU	SWMKA	CCLAY	QKNFC
Ciphertext:	MWMHT	TFYQS	TLTMG	PUSWM	KACCL	AYQKN	FCHOL	TOEKW

Playfair (First Digraph Cipher)

- Key:

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

- plaintext: HI DE TH EG OL DI NT HE TR EX ES TU MP
- ciphertext: BM ND ZB XD KY BE JV DM UI XM MN UV IF

Hill Cipher

- polygraphic substitution cipher based on linear algebra

Consider the message 'ACT', and the key below (or GYBNQKURP in letters):

$$\begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix}$$

Since 'A' is 0, 'C' is 2 and 'T' is 19, the message is the vector:

$$\begin{pmatrix} 0 \\ 2 \\ 19 \end{pmatrix}$$

Thus the enciphered vector is given by:

$$\begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix} \begin{pmatrix} 0 \\ 2 \\ 19 \end{pmatrix} = \begin{pmatrix} 67 \\ 222 \\ 319 \end{pmatrix} \equiv \begin{pmatrix} 15 \\ 14 \\ 7 \end{pmatrix} \pmod{26}$$

which corresponds to a ciphertext of 'POH'. Now, suppose that our message is instead 'CAT',

KASISKI METHOD

- The Kasiski analysis first finds the length of the keyword used in the polyalphabetic substitution cipher. Then lines up the ciphertext in *n* columns, where *n* is the length of the keyword. Then, each column can be treated as the ciphertext of a monoalphabetic substitution cipher. As such, each column can be attacked with frequency analysis.

KASISKI ANALYSİS

- It is given that the following ciphertext is obtained by Keyword Vigenere cryptosystem.

  SDMXG GVTWB QBTIU QUTYK GSVMH ZGXZQ LJBTG JGIXV PKSIZ MYNIE BLBFMKVWQ NMIMR IWRVS XOIWG GVYTQ PYGGS TLWGJ ELJIZ RCRMO JIEQJ ZQTICWRUJM WVPXZ GAEZG PGEIX VQRGP MEPJG STLQN MIKWZ ILQYF QBIJJ MUJMRQKWMR WRRCG ZQNXU GGSTL XBGRK WZICT SHGZS EKIFV IXVQR

- Most frequent triples and quadrapules are as follows:

GGV:2/ 70	QNM:2/ 84	GGS:2/ 98
STL:3/ 56,42	XVQ:2/ 77	KWZ:2/ 42
QNMI:2/ 84	GSTL:3/ 56,42	XVQR:2/ 77
IXV:3/ 91,77	NMI:2/ 84	GST:3/ 56,42
UJM:2/ 49	VQR:2/ 77	WZI:2/ 42
GGST:2/ 98	IXVQ:2/ 77	KWZI:2/ 42

- One can easily suggest that the key length is 7. Then we rewrite the cipher text in 7 columns. We also write the most frequent letter in each column:

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

- Since the most frequent letters in English are E, T, A, and O, we first consider the case he above letters are images of these letters.
- For example, if E is mapped to S in the first column, then the first letter of the key must be O. Considering all possibilities we get the following table:

Most Frequent Letter in the column	S	Q	I	X		G	G
Letter of the key if preimage is E	O	M	E	T		C	C
Letter of the key if preimage is T	Z	X	P	E		J	J
Letter of the key if preimage is A	S	Q	I	X		G	G
Letter of the key if preimage is O	E	C	U	J		S	S

- Among all these letters, the G in 6th column repeats 7 times. So we start by assuming that the 6th letter of the key is C. Then the 6th column of the plain text is

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

- Last letter of key, most probably, is not C. So we may try replacing I and R, each of which appears five times in the last row, with E. Replacing I with E gives RE, LE, LE, KE, IE and replacing R with E gives AE, UE, OE, EE, OE. It seems reasonable to replace I with E which means that the last letter of the key is E. Then, we get

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

- There are four V in the 5th column and they stand as vNG, vNT, vON. So, it most be a vowel. Possibilities are ANG ANT AON, ENG ENT EON, ING INT ION, ONG ONT OON, UNG UNT UON. It is reasonable to try replacing V with I which means that the 5th letter of the key is N:
- Moreover we have two I's in the third column and two X's in the fourth column preceding vON (ION) so I must correspond to A and X must correspond T. This means that the third letter is I and fourth letter is E. Then with this substitutions we have

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

- Now, considering the frequency table above, we can suggest that the key is SCIENCE

TRANSPOSITION CIPHERS

- A transposition (or permutation) cipher hides the message contents by rearranging the order of the letters.
- The key is a permutation expressed usually as a word or phrase. We assign a number to each letter in the word using the following rule:
  - the numbers are assigned starting with 1, and they are assigned first by alphabetical order,
  - Thus C R A Z Y B I R D gives the permutation 3 6 1 9 8 2 5 7 4.

Transposistion Ciphers(Cont.)

- Since a transposition cipher just permutes the letters of a message, at least for long texts, a frequency count will show a normal language profile.
- Basic idea in cryptanalysis of transposition Ciphers is to guess the period (the key length), then to look at all possible permutations in period, and search for common patterns.

Rail Fence Cipher

- The message is written with letters on alternate k rows then the ciphertext is read off row by row. The number k is called the depth.

```
Depth 5: B       E       E       R       W       L       L       O
          I     V W     R A     N I     A O     U G     A L     N A
           R   O   H   B   D   W   C   D   N   F   R   C   E   I
            D L     E T     B O     E N     D R     A N     D U
             S       A       R       A       E       I       Q
```

Ciphertext: BEERW LLOIV WRANI AOUGA LNARO HBDWC DNFRC EIDLE TBOEN DRAND USARA EIQ

Red Fence cipher

- Only difference of this cipher from the rail fence is that the order of the rows in writing the ciphertext is determined by a key. Consider the depth 5 rail fence given above.
- Key: 34152

```
Depth 5: B       E       E       R       W       L       L       O
          I     V W     R A     N I     A O     U G     A L     N A
           R   O   H   B   D   W   C   D   N   F   R   C   E   I
            D L     E T     B O     E N     D R     A N     D U
             S       A       R       A       E       I       Q
```

- Ciphertext: ROHBD WCDNF RCEID LETBO ENDRA NDUBE ERWLL OSARA EIQIV WRANI AOUGA LNA

Simple (Column/Row) Transposition Cipher

- Write in the message under the keyword in a number of columns. Then, arrange the columns in numerical order, and write across the ciphertext.

Simple Trans.Cipher (Cont.)

Key: L O V E B I R D (5 6 8 3 1 4 7 2)

Plain text

		L	O	V	E	B	I	R	D
		5	6	8	3	1	4	7	2
L	5	B	I	R	D	S	L	O	V
O	6	E	W	H	E	A	T	B	R
V	8	E	A	D	B	R	O	W	N
E	3	R	I	C	E	A	N	D	A
B	1	W	O	N	D	E	R	F	U
I	4	L	G	R	A	I	N	C	A
R	7	L	L	E	D	Q	U	I	N
D	2	O	A						

Columns Permuted

		B	D	E	I	L	O	R	V
		1	2	3	4	5	6	7	8
L	5	S	V	D	L	B	I	O	R
O	6	A	R	E	T	E	W	B	H
V	8	R	N	B	O	E	A	W	D
E	3	A	A	E	N	R	I	D	C
B	1	E	U	D	R	W	O	F	N
I	4	I	A	A	N	L	G	C	R
R	7	Q	N	D	U	L	L	I	E
D	2					O	A		

Decryption consists of writing the message out in columns and reading off the message by reordering columns. For example, the decryption key of the above example is 5 8 4 6 1 2 7 3 which is the inverse (permutation) of the encryption permutation 5 6 8 3 1 4 7 2.

Ciphertext:

SVDLB IORAR ETEWB HRNBO EAWDA AENRI DCEUD RWOFN IAANL GCRQN DULLI EOA

Ciphertext (Columns permuted) Broken Diagonals /:
SVADRRLENABTBAEIEOEUIOWENDAQRBARRANHWIWNDDDOLUCFGLNCLORIAE

Nihilist Cipher

- A more complex transposition cipher using both row and column transpositions is the nihilist cipher. The message is written in rows then both rows and columns are permuted in order controlled by the key. Then ciphertext is read off by rows or columns.

Nihilist Cipher

Plain text

		L	O	V	E	B	I	R	D
		5	6	8	3	1	4	7	2
L	5	B	I	R	D	S	L	O	V
O	6	E	W	H	E	A	T	B	R
V	8	E	A	D	B	R	O	W	N
E	3	R	I	C	E	A	N	D	A
B	1	W	O	N	D	E	R	F	U
I	4	L	G	R	A	I	N	C	A
R	7	L	L	E	D	Q	U	I	N
D	2	O	A						

Columns and rows permuted

		B	D	E	I	L	O	R	V
		1	2	3	4	5	6	7	8
B	1	E	U	D	R	W	O	F	N
D	2					O	A		
E	3	A	A	E	N	R	I	D	C
I	4	I	A	A	N	L	G	C	R
L	5	S	V	D	L	B	I	O	R
O	6	A	R	E	T	E	W	B	H
R	7	Q	N	D	U	L	L	I	E
V	8	R	N	B	O	E	A	W	D

Ciphertext (Read off by rows):

EUDRW OFNOA AAENR IDCIA ANLGC RSVDL BIORA RETEW BHQND ULLIE RNBOE AWD

Ciphertext (Read off by columns):

EAISA QRUAA VRNND EADED BRNNL TUOWO RLBEL EOAIG IWLAF DCOBI WNCRR HED

Sacco Cipher

- This is a variant of columnar transposition that produces a different cipher. Here, the first row is filled in only up to the column with the key number 1; the second row is filled in only up to the column with the key number 2; and so on. Period is k(k+1)/k where k is the length of the key: the matrix can hold at most k(k+1)/2 letters, so first k(k+1)/2 letters of the plaintext is encrypted then next k(k+1)/2 letters and so on.

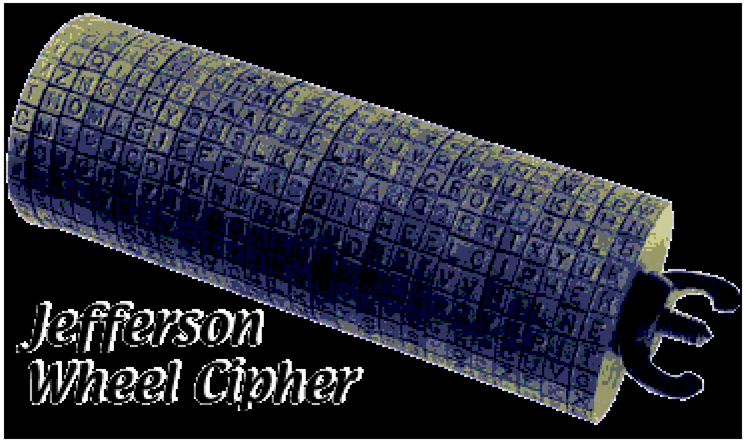
Sacco Cipher(cont.)

L O V E B I R D
5 6 8 3 1 4 7 2

B I R D S
L O V E W H E A
T B R E
A D B R O W
N
R I
C E A N D A W
O N D
E R F U L
G R A I N C A L
L E D Q
U I N O A

Ciphertext: SWODA DEERN HWABL TANRC OIOBD IENEW RVRBN LNALU IQOCE GLURR EIAFA DN

Jefferson Wheel Cipher



JEFFERSON WHEELS

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
N	J	E	N	J	L	E	A	L	A	G	L	J	A	G	E	N	G	N	E	L	G	J	A	A
H	P	X	U	G	M	D	L	H	O	U	N	A	B	P	M	V	N	S	L	C	R	I	V	Y
Z	D	B	P	W	D	P	X	O	E	Q	W	K	C	E	W	T	X	W	Z	K	C	Q	Q	S
J	F	O	J	F	Z	O	D	Z	D	W	Z	F	D	W	O	J	W	J	O	Z	W	F	D	D
W	O	P	Z	D	O	Z	Q	Q	X	S	D	W	E	X	T	B	Q	T	W	W	E	K	S	C
K	B	A	K	B	S	A	J	S	J	T	R	V	F	Z	C	Y	T	Y	C	R	Z	V	F	F
E	L	N	E	L	J	N	G	J	G	A	J	L	G	A	N	E	A	E	N	J	A	L	G	G
Q	A	M	V	I	C	F	B	N	Y	P	U	X	H	I	D	H	R	U	X	H	U	P	O	L
D	N	V	X	C	G	Q	P	P	R	L	A	U	I	B	H	M	O	L	U	I	Y	H	N	U
Y	V	C	Y	V	R	C	F	R	F	Z	S	B	J	T	A	K	Z	K	A	S	T	B	J	J
G	X	D	H	P	H	R	H	U	L	I	E	T	K	M	F	Q	U	V	M	N	P	A	Y	B
V	I	L	S	Y	T	M	Y	C	V	R	H	P	L	U	X	U	K	R	I	M	N	G	M	O
F	U	H	M	H	I	G	I	A	U	B	X	E	M	H	Q	D	Y	X	V	P	L	N	R	P
I	T	F	Q	A	N	S	K	E	B	M	Y	M	N	V	R	G	P	H	D	U	I	X	L	H
S	Y	G	F	U	A	L	V	T	I	K	M	G	O	N	I	R	B	D	Q	X	H	E	P	M
M	H	U	L	M	Y	H	U	I	N	Y	P	N	P	L	V	X	V	I	S	G	O	C	K	R
B	K	W	T	Q	K	T	C	W	S	E	Q	O	Q	S	P	Z	C	P	B	O	Q	D	E	X
L	M	R	G	X	U	U	N	Y	H	V	G	C	R	O	S	I	I	Q	F	E	M	T	B	K
P	W	T	B	K	W	B	E	D	C	X	K	Q	S	C	Z	W	E	Z	P	Q	S	O	X	Q
A	R	Y	A	R	B	Y	Z	B	Z	J	V	S	T	F	K	C	J	C	K	V	F	S	T	T
X	C	S	I	T	E	V	R	G	K	O	I	H	U	Y	U	L	M	G	R	Y	V	M	H	N
R	E	Q	D	N	P	I	M	X	P	H	T	Y	V	K	G	F	L	M	H	A	B	U	U	I
O	Z	J	O	Z	F	J	W	F	W	D	F	Z	W	D	J	O	D	O	J	F	D	Z	W	W
T	Q	Z	W	O	Q	W	S	K	Q	C	O	D	X	Q	B	P	S	B	T	D	X	W	C	E
U	G	I	R	E	X	X	O	M	M	N	C	I	Y	R	L	S	H	F	G	T	K	Y	I	V
C	S	K	C	S	V	K	T	V	T	F	B	R	Z	J	Y	A	F	A	Y	B	J	R	Z	Z

Disks are arranged according to the give permutation:Key Permutation: 14,7,13,15,1,12,8,16,2,11,17,9,25,3,23,22,4,21,10,20,5,18,19,6,24

14	7	13	15	1	12	8	16	2	11	17	9	25	3	23	22	4	21	10	20	5	18	19	6	24
A	E	J	G	N	L	A	E	J	G	N	L	A	E	J	G	N	L	A	E	J	G	N	L	A
B	D	A	P	H	N	L	M	P	U	V	H	Y	X	I	R	U	C	O	L	G	N	S	M	V
C	P	K	E	Z	W	X	W	D	Q	T	O	S	B	Q	C	P	K	E	Z	W	X	W	D	Q
D	O	F	W	J	Z	D	O	F	W	J	Z	D	O	F	W	J	Z	D	O	F	W	J	Z	D
E	Z	W	X	W	D	Q	T	O	S	B	Q	C	P	K	E	Z	W	X	W	D	Q	T	O	S
F	A	V	Z	K	R	J	C	B	T	Y	S	F	A	V	Z	K	R	J	C	B	T	Y	S	F
G	N	L	A	E	J	G	N	L	A	E	J	G	N	L	A	E	J	G	N	L	A	E	J	G
H	F	X	I	Q	U	B	D	A	P	H	N	L	M	P	U	V	H	Y	X	I	R	U	C	O
I	Q	U	B	D	A	P	H	N	L	M	P	U	V	H	Y	X	I	R	U	C	O	L	G	N
J	C	B	T	Y	S	F	A	V	Z	K	R	J	C	B	T	Y	S	F	A	V	Z	K	R	J
K	R	T	M	G	E	H	F	X	I	Q	U	B	D	A	P	H	N	L	M	P	U	V	H	Y
L	M	P	U	V	H	Y	X	I	R	U	C	O	L	G	N	S	M	V	I	Y	K	R	T	M
M	G	E	H	F	X	I	Q	U	B	D	A	P	H	N	L	M	P	U	V	H	Y	X	I	R
N	S	M	V	I	Y	K	R	T	M	G	E	H	F	X	I	Q	U	B	D	A	P	H	N	L
O	L	G	N	S	M	V	I	Y	K	R	T	M	G	E	H	F	X	I	Q	U	B	D	A	P
P	H	N	L	M	P	U	V	H	Y	X	I	R	U	C	O	L	G	N	S	M	V	I	Y	K
Q	T	O	S	B	Q	C	P	K	E	Z	W	X	W	D	Q	T	O	S	B	Q	C	P	K	E
R	U	C	O	L	G	N	S	M	V	I	Y	K	R	T	M	G	E	H	F	X	I	Q	U	B
S	B	Q	C	P	K	E	Z	W	X	W	D	Q	T	O	S	B	Q	C	P	K	E	Z	W	X
T	Y	S	F	A	V	Z	K	R	J	C	B	T	Y	S	F	A	V	Z	K	R	J	C	B	T
U	V	H	Y	X	I	R	U	C	O	L	G	N	S	M	V	I	Y	K	R	T	M	G	E	H
V	I	Y	K	R	T	M	G	E	H	F	X	I	Q	U	B	D	A	P	H	N	L	M	P	U
W	J	Z	D	O	F	W	J	Z	D	O	F	W	J	Z	D	O	F	W	J	Z	D	O	F	W
X	W	D	Q	T	O	S	B	Q	C	P	K	E	Z	W	X	W	D	Q	T	O	S	B	Q	C
Y	X	I	R	U	C	O	L	G	N	S	M	V	I	Y	K	R	T	M	G	E	H	F	X	I
Z	K	R	J	C	B	T	Y	S	F	A	V	Z	K	R	J	C	B	T	Y	S	F	A	V	Z

Disks are rotated so that the plain text appears in a row, then any of the other rows can be used as the cryptotext.

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

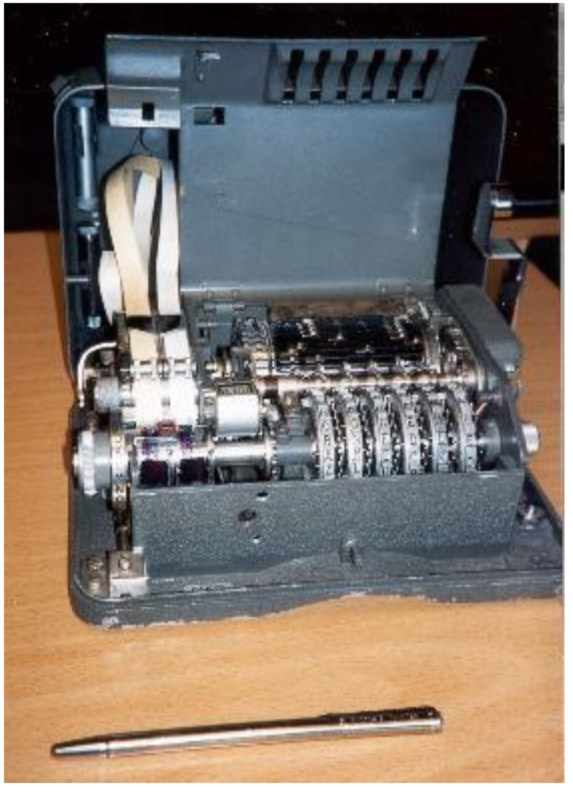
Product Ciphers

- ciphers using substitutions or transpositions are not secure because of language characteristics
- hence consider using several ciphers in succession to make harder, but:
  - two substitutions make a more complex substitution
  - two transpositions make more complex transposition
  - but a substitution followed by a transposition makes a new much harder cipher
- this is bridge from classical to modern ciphers

Rotor Machines

- before modern ciphers, rotor machines were most common complex ciphers in use
- widely used in WW2
  - German Enigma, Allied Hagelin, Japanese Purple
- implemented a very complex, varying substitution cipher
- used a series of cylinders, each giving one substitution, which rotated and changed after each letter was encrypted
- with 3 cylinders have 26^3=17576 alphabets

Hagelin Rotor Machine



Hagelin: The **C-35** and **C-36** were cipher machines designed by Swedish cryptographer Boris Hagelin in the 1930s. These were the first of Hagelin's cipher machines to feature the pin-and-lug mechanism. A later machine in the same series, the M-209, was widely-used by the United States military.

Modern Ciphers

- Bigger and bigger keys
- More and more complicated algorithms
- Based on hardcore applied mathematics... and the difficulty of factoring large numbers

Steganography

- an alternative to encryption
- hides existence of message
  - using only a subset of letters/words in a longer message marked in some way
  - using invisible ink
  - hiding in LSB in graphic image or sound file
- has drawbacks
  - high overhead to hide relatively few info bits
- advantage is can obscure encryption use

Historic techniques

- Invisible ink
- Tatoo message on head
- Pin punctures in type
- Microdots ..

Motivation

- Steganography received little attention in computing
- Renewed interest because of industry desire to protect copyrighted digital work
  - audio
  - images
  - video
  - Text
- Detect counterfeiter, unauthorized presentation, embed key, embed author ID
- Steganography ≠ Copy protection

Null Cipher

- Hide message among irrelevant data
- Confuse the cryptoanalyst

Big rumble in New Guinea.
The war on
celebrity acts should end soon.
Over four
big ecstatic elephants replicated.

Bring two cases of beer.

Thousands of years ago, the Greeks used steganography to hide information from their enemies.

One hiding method was to engrave a message in a block of wood, then cover it with wax, so it looked like a blank wax tablet. When they wanted to retrieve the message, they would simply melt off the wax.

*diit.sourceforge.net/files/**OpenDay2006v2**.ppt*

You can try steganography at home by writing on a piece of paper with lemon juice.

If you heat the paper with a hair dryer the juice will burn and reveal the hidden message.

Note for those who wish to try this at home: Paper burns too, so stop heating the paper before it catches fire!

Pictures are made up of lots of little dots called pixels. Each pixel is represented as 3 bytes – one for red, one for green and one for blue.

11111000 11001001 00000011

248 201 3

Each byte is interpreted as a number, which is how much of that colour is used to make the final colour of the pixel.

248 + 201 + 3 = Orange Colour

The difference between two colours that differ by one in either one red, green or blue value is impossible to see with the human eye.

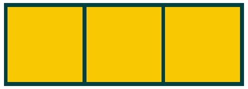
248	**201**	**3**	**Original Colour**
248	**201**	**4**	**Blue +1**
247	**201**	**3**	**Red -1**

If we change **the least significant (last) bit in a byte, we either add or subtract one from the value it represents.**

This means we can overwrite the last bit in a byte without affecting the colour it appears to be.

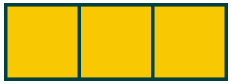
We can use images to hide things if we replace the last bit of every colour’s byte with a bit from the message.

Message: A 01000001

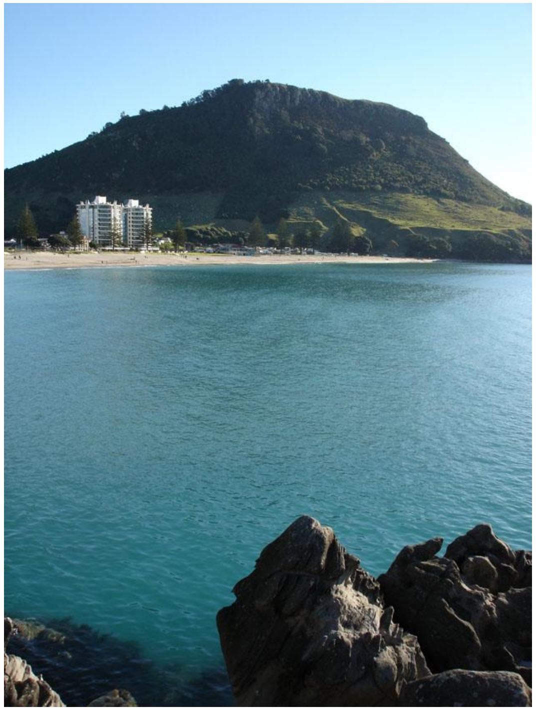
Image with 3 pixels: 

Pixel 1:	11111000	11001001	00000011
Pixel 2:	11111000	11001001	00000011
Pixel 3:	11111000	11001001	00000011

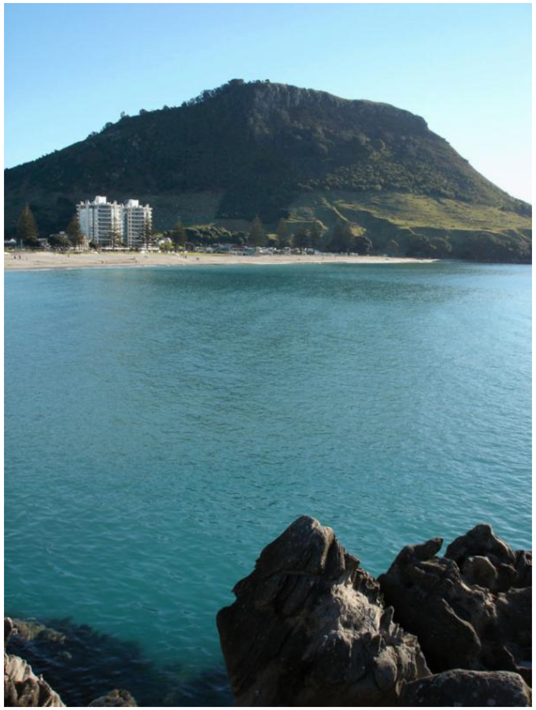
Pixel 1:	11111000	11001001	00000010
Pixel 2:	11111000	11001000	00000010
Pixel 3:	11111000	11001001	00000011

New image: 

Even if we do this across a big image and with a really large message, it is still hard to tell that anything is wrong.



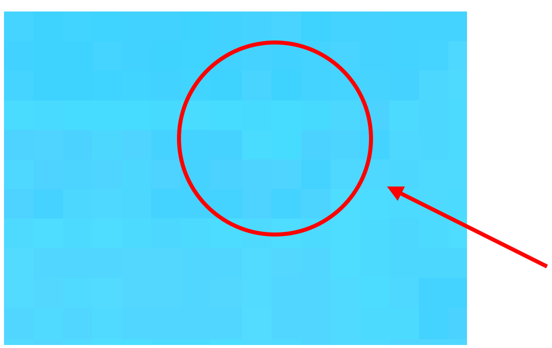
Original



With Hidden Message

Normally when we hide a message in an image we just start at the top left pixel and keep writing across the image until we are done.

This may appear to work quite well, but if we zoom right in and look at the pixels in a block of plain colour then we can see that some pixels aren’t all the same.



Plain blue sky from image of the Mount

Look here

If we change an edge it is harder to notice because two pixels next to each other will already have very different colours.

So what we want to do is hide in the edges of a picture because then we can avoid hiding in blocks of colour.

Image we want to hide a message in

Where we want to hide the message

Can you pick the picture with the hidden message?

http://diit.sourceforge.net