CSEC
CYBER SECURITY EDUCATION CONSORTIUM

Encryption & Decryption – 1

Sujeet Shenoi
Tandy School of Computer Science
University of Tulsa, Tulsa, OK 74104
sujeet@utulsa.edu

NSF

ADVANCED TECHNOLOGICAL EDUCATION

CSEC
CYBER SECURITY EDUCATION CONSORTIUM

Fundamentals

Message

- Sender, Receiver, Transmission Medium
- Plaintext (P), Ciphertext (C)
- Interceptor/Intruder
  - Block message (Interruption)
  - Access message (Interception)
  - Modify message (Modification)
  - Fabricate message (Fabrication)

ADVANCED TECHNOLOGICAL EDUCATION

Fundamentals (contd.)

Cryptography

- Using encryption to conceal plaintext

Cryptanalysis

- Unauthorized "code breaking"

Cryptology

- Cryptography and Cryptanalysis

Fundamentals (contd.)

Breakable Encryption

- Analysts can determine the algorithm given enough time and data
- Theoretically breakable; Practically unbreakable
- Brute force attacks
- Ingenious attacks
- Estimates of breakability based on current technology (Moore's Law: Processor speed doubles every 1.5 years)

Basic Encryption/Decryption

Key-Based Ciphers

- Provide more security (than Keyless Ciphers)
- Encryption Key (K_E); Decryption Key (K_D)
- $C = \{ P \}_{K_E}$
- $P = \{ C \}_{K_D} = \{ \{ P \}_{K_E} \}_{K_D}$
- Symmetric Encryption: $K_E = K_D$
- Asymmetric Encryption: $K_E \neq K_D$

Symmetric Encryption

Secret Key/Private Key Encryption

- $K_E = K_D$
- One key per channel
- n users: ½·n· (n−1) channels/keys
- Authentication (if key is kept secret)
- Key distribution is problematic
- Key management is always an issue (storing, safeguarding and activating keys)

Asymmetric Encryption

Private Key Encryption

- $K_E \neq K_D$
- Two keys per user (K_A^{priv} & K_A^{pub})
- n users: 2·n keys
- Authentication (if K_A^{priv} is kept secret)
- Key management is simplified, but is an issue

Basic Cipher Types

- Substitution Ciphers
  - Replace each plaintext character with another character
- Transposition Ciphers
  - Scramble or shuffle plaintext characters

Substitution Ciphers

Monoalphabetic Ciphers

- Single alphabet is used for substitution
- Caesar Cipher
  - Plaintext Alphabet: `ABCDEF…UVWXYZ`
  - Ciphertext Alphabet: `defghi…xyzabc`

  - Plaintext: `WEATT ACKAT DAWNX`
  - Ciphertext: `zhdww dfndw gdzqa`

Monoalphabetic Ciphers

Monoalphabetic Ciphers

- Key-Based Cipher
  - Plaintext Alphabet: `ABCDEFGHI…UVWXYZ`
  - Ciphertext Alphabet: `keyabcdfg…tuvwxz`
- Substitution Cipher ($\Pi(\lambda) = (3 \cdot \lambda) \bmod 26$)
  - Plaintext Alphabet: `ABCDEFGHI…UVWXYZ`
  - Ciphertext Alphabet: `adgjmpsvy…ilorux`

Monoalphabetic Ciphers (contd.)

Breaking Monoalphabetic Ciphers

- Frequency Distributions
  - Each language has a characteristic distribution
  - Index of Coincidence (English IC = 0.068)
  - Computers make code breaking trivial
- Solution: "Flatten Frequency Distributions"
- Polyalphabetic Ciphers (multiple alphabets)

Monoalphabetic Ciphers (contd.)

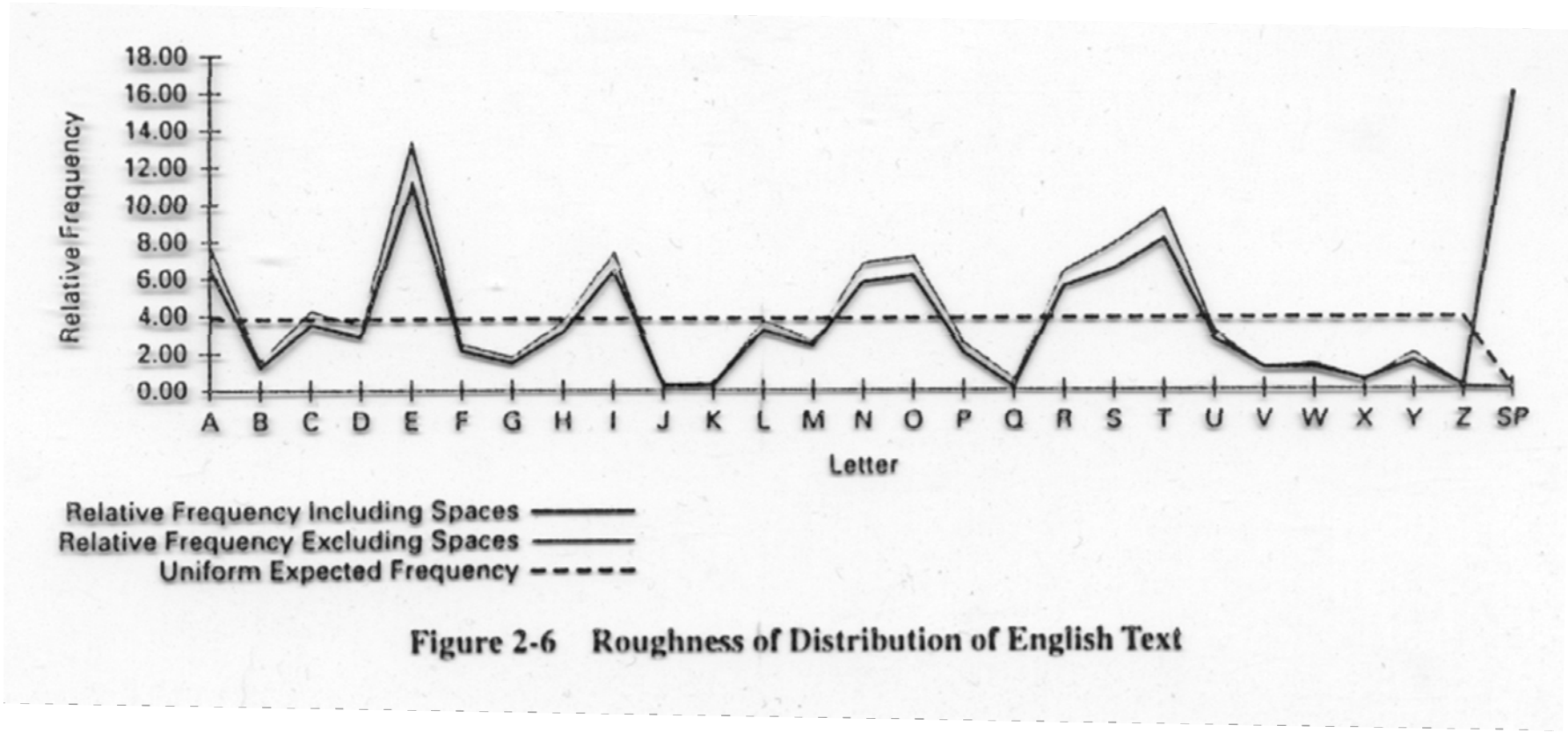


Figure 2-6 Roughness of Distribution of English Text

Polyalphabetic Ciphers

Polyalphabetic Ciphers

- Multiple alphabets flatten distributions
  - 26! possible alphabets

#Alphabets:	1	2	3	4	5	10	∞
IC	0.068	0.052	0.047	0.044	0.044	0.041	0.038

- Example
  - T H I S I S A T E S T X X X X
  - π_1 π_2 π_3 π_1 π_2 π_3 π_1 π_2 π_3 π_1 π_2 π_3 π_1 π_2 π_3
  - Choose π_1 π_2 π_3 so that frequencies are flat

Polyalphabetic Ciphers (contd.)

Vigenère Cipher

- Polyalphabetic cipher based on Vigenère Tableau
- 26 possible alphabets, each "keyed" by a letter
- Example
  - Key: *julie tjuli et*
  - Plaintext: BUTSO FTWHA TL
  - Ciphertext: koeas ycqsi …

Polyalphabetic Ciphers (contd.)

Table 2-5 Vigenère Tableau

	0					5					10					15					20					25	
	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	π
A	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	0
B	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	a	1
C	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	2
D	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	3
E	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	4
F	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	5
G	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	6
H	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	7
I	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	8
J	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	9
K	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	10
L	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	11
M	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	12
N	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	13
O	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	14
P	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	15
Q	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	16
R	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	17
S	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	18
T	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	19
U	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	20
V	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	21
W	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	22
X	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	23
Y	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	24
Z	z	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	25

Polyalphabetic Ciphers (contd.)

```
julie tjuli etjul ietju lietj uliet julie tjuli
BUTSO ETWHA TLIGH TTHRO UGHYO NDERW INDOW BREAK
koeas ycqsi ...
```

```
dicke nsdic kensd icken sdick ensdi ckens dicke
ITWAS THEBE STOFT IMESI TWAST HEWOR STOFT IMESI

nsdic kensd icken sdick ensdi ckens dicke nsdic
TWAST HEAGE OFWIS DOMIT WASTH EAGEO FFOOL ISHNE

kensd icken sdick ensdi ckens dicke nsdic kensd
SSITW ASTHE EPOCH OFBEL IEFIT WASTH EEPOC HOFIN
```

Starting Position	Distance from Previous	Factors
20		
83	63 (83 – 20)	3, 7, 9, 21, 63
104	21 (104 – 83)	3, 7, 21

Polyalphabetic Ciphers (contd.)

Breaking Ciphers (Kasiski's Method):

- K: *dicke nsdic kensd icken sdick ensdi ckens dicke*
- P: ITWAS THEBE STOFT IMESI TWAST HEWOR STOFT IMESI

20

- K: *nsdic kensd icken sdick ensdi ckens dicke nsdic*
- P: TWAST HEAGE OFWIS DOMIT WASTH EAGEO FFOOL ISHNE

- K: *kensd icken sdick ensdi ckens dicke nsdic kensd*
- P: SSITW ASTHE EPOCH OFBEL IEFIT WASTH EEPOC HOFIN

83 (dist: 63; factors: 3,7,9,21,63) 104 (dist: 21; factors: 3,7,21)

Polyalphabetic Ciphers (contd.)

	a	*e*	*i*	*n*	*o*	*t*
A	a	e	i	n	o	t
E	e	l	m	r	s	x
I	i	m	r	w	x	c
N	n	r	w	b	c	h
O	o	s	x	c	d	l
T	t	x	b	g	h	m

This table is more useful "inside out": a could represent A, b could stand for N or T, and so on.

Searching through this table for possibilities, we transform the cryptogram.

Ciphertext	u	a	o	p	m		k	m	k	v	t		u	n	h	b	l		j	m	e	d
Possible plaintexts	?	**A**	A	?	E		?	**E**	?	?	**A**		?	A	N	N	?		?	E	A	?
			O		**I**			I			T			**N**	T	**T**				**I**	E	
					T			T												T		

Polyalphabetic Ciphers (contd.)

V	E	R	N	A	M	C	I	P	H	E	R
21	4	17	13	0	12	2	8	15	7	4	17

Next we need some random numbers to combine with the letter codes. Suppose the following series of random two-digit numbers is generated.

76 48 16 82 44 03 58 11 60 05 48 88

The encoded form of the message is the sum mod 26 of each coded letter with the corresponding random number. The result is then encoded in the usual base-26 alphabet representation.

Plaintext	V	E	R	N	A	M	C	I	P	H	E	R
Numeric Equivalent	21	4	17	13	0	12	2	8	15	7	4	17
+ Random Number	76	48	16	82	44	3	58	11	60	5	48	88
= Sum	97	52	33	95	44	15	60	19	75	12	52	105
= mod 26	19	0	7	17	18	15	8	19	23	12	0	1
Ciphertext	t	a	h	r	s	p	i	t	x	m	a	b

Thus, the message

VERNAM CIPHER

is encoded as

tahrsp itxmab

Perfect Substitution Ciphers

01001010100101010101010011001010101010000101010101010101010100010100100

Infinite non-repeating sequences of alphabets
(Immunity to Kasiski's Method)

- One-Time Pad
- Long Random Number Sequences
- Vernam Cipher (punched paper tape)
- Book Ciphers (e.g., Telephone Book, Bible)

Perfect Substitution Ciphers (contd.)

- Dual Message Entrapment
  - Key: `disre gardt hisme ssage`
  - Message: `THISM ESSAG EISCR UCIAL`

Transposition Ciphers

Columnar Transposition

- Example (c = 10)

```
T H I S I S A M E S
S A G E T O S H O W
H O W A T R A N S P
O S I T I O N C I P
H E R W O R K S X X
```

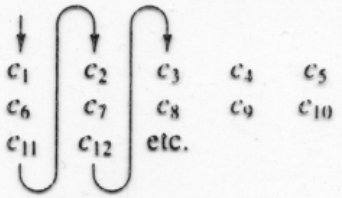
- Ciphertext

```
TSHOH HAOSE IGWIR SEATW ITTIO SOROR ASANK
MHNCS EOSIX SWPPX
```

Transposition Ciphers (contd.)

c_1	c_2	c_3	c_4	c_5
c_6	c_7	c_8	c_9	c_{10}
c_{11}	c_{12}	etc.		

The resulting ciphertext is formed by traversing the columns.



As an example, you would write the plaintext message as

T	H	I	S	I
S	A	M	E	S
S	A	G	E	T
O	S	H	O	W
H	O	W	A	C
O	L	U	M	N
A	R	T	R	A
N	S	P	O	S
I	T	I	O	N
W	O	R	K	S

The resulting ciphertext would then be read as

```
tssoh oaniw haaso lrsto imghw
utpir seeoa mrook istwc nasns
```

Transposition Ciphers (contd.)

Breaking Transposition Ciphers

- Common Digrams and Trigrams
- Digrams: EN, RE, ER, NT, TH, ON, IN, TE, AN, OR
- Trigrams: ENT, ION, AND, ING, IVE, TIO, FOR, OUR, THI, ONE
- Sliding Window Technique

```
TSH
   OHH      AOSEIGWIRSEATWITTIOSORORASANKMHNCSEOSIXSWPPX
TSHO
   HHAO     SEIGWIRSEATWITTIOSORORASANKMHNCSEOSIXSWPPX
TSHOH
   HAOSE    IGWIRSEATWITTIOSORORASANKMHNCSEOSIXSWPPX
```

Transposition Ciphers (contd.)

0100101010010101010101001100101010101000010101010101010101000010100100

Table 2-7 Most Common Digrams and Trigrams

Digrams	Trigrams
EN	ENT
RE	ION
ER	AND
NT	ING
TH	IVE
ON	TIO
IN	FOR
TF	OUR
AN	THI
OR	ONE

Transposition Ciphers (contd.)

Table 2-8 Frequencies per 10,000 Characters of Digrams in English Example

	A	B	C	D	E	F	G	H	I	J	K	L	M
A	0.0	19.2	41.3	11.4	0.1	3.7	10.2	0.6	13.9	0.6	4.7	70.7	19.0
B	5.6	0.0	0.0	0.1	35.7	0.0	0.0	0.0	7.0	13.1	0.0	19.8	0.4
C	42.5	1.6	15.1	0.1	56.1	0.1	0.0	37.1	14.5	0.0	5.9	10.3	0.0
D	11.7	0.1	0.0	3.4	73.6	0.0	0.8	0.0	26.7	0.0	0.0	0.8	0.6
E	39.3	0.5	80.9	70.4	16.1	12.9	8.6	0.6	5.9	0.1	0.3	41.2	37.8
F	8.6	0.0	0.0	0.0	17.7	14.2	0.0	0.0	25.5	0.0	0.0	3.8	0.0
G	6.6	0.0	0.0	0.0	19.2	0.1	0.4	11.4	7.6	0.0	0.0	1.6	0.8
H	50.4	0.0	0.0	0.0	146.4	0.1	0.0	0.1	24.7	0.0	0.0	0.4	0.5
I	16.9	8.4	43.4	17.4	18.6	21.7	32.7	0.0	0.0	0.0	1.3	22.5	27.8
J	0.0	0.0	0.0	0.0	16.1	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
K	0.5	0.0	0.0	0.0	10.5	0.0	0.0	0.0	2.8	0.0	0.0	0.1	0.0
L	32.1	0.1	0.2	7.9	65.7	0.6	0.5	0.0	30.6	0.0	0.1	30.6	0.3
M	33.9	4.8	0.1	0.3	62.3	0.0	0.0	0.0	15.9	0.0	0.0	0.4	7.3
N	20.2	0.2	28.5	67.8	41.4	9.7	58.5	0.5	21.1	0.1	0.9	3.5	2.2
O	1.8	10.3	11.6	21.3	2.0	67.7	8.5	0.1	2.4	2.9	2.3	20.4	35.5
P	19.4	0.1	0.2	0.1	48.4	0.2	0.0	2.7	2.7	0.0	0.0	24.6	1.6
Q	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
R	52.0	0.1	12.4	7.8	132.3	3.0	5.1	0.3	75.2	0.0	2.7	2.4	18.6
S	8.1	0.0	7.8	0.2	97.2	1.8	0.0	10.2	52.5	0.0	1.7	1.4	4.2
T	37.5	0.0	3.8	0.2	101.5	0.3	0.0	196.8	121.0	0.0	0.0	2.7	4.4
U	16.8	8.3	13.5	7.7	9.9	0.5	3.6	0.0	6.9	0.0	0.0	24.4	6.1
V	17.0	0.0	0.0	0.0	51.5	0.0	0.0	0.0	20.3	0.0	0.0	0.0	0.5
W	12.6	0.0	0.1	0.0	19.2	0.0	0.0	16.2	16.7	0.0	0.0	0.2	0.0
X	6.4	0.0	0.3	0.0	1.9	0.0	0.0	0.1	1.8	0.0	0.0	0.0	0.0
Y	0.2	0.1	0.1	0.2	2.6	0.0	0.0	0.0	1.7	0.0	0.0	0.0	0.2
Z	3.2	0.0	0.0	0.0	4.6	0.0	0.0	0.0	0.3	0.0	0.0	0.0	0.0
SP	201.1	60.0	98.4	65.4	63.9	64.0	12.4	27.8	120.7	2.2	7.1	31.4	58.2

Transposition Ciphers (contd.)

	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	SP
A	119.1	0.00	10.9	0.0	65.9	49.8	118.8	6.6	9.8	1.8	0.9	9.6	0.0	55.8
B	0.0	4.5	0.0	0.0	1.9	1.8	0.6	7.5	0.3	0.0	0.0	8.2	0.0	7.4
C	0.0	57.4	0.0	0.1	11.7	2.4	63.2	28.5	0.0	0.0	0.0	3.0	0.0	126.6
D	0.1	11.0	0.0	0.0	2.0	5.8	0.1	12.5	1.1	1.6	0.0	3.0	0.0	126.6
E	99.2	2.0	13.3	8.0	143.0	132.0	26.4	1.8	27.0	3.1	28.9	4.4	0.0	310.9
F	0.0	37.2	0.0	0.0	8.2	0.2	5.3	7.7	0.0	0.0	0.0	1.9	0.0	70.2
G	16.6	3.5	0.0	0.0	12.8	1.0	0.5	8.5	0.0	0.0	0.0	0.5	0.0	50.4
H	3.2	23.4	0.0	0.0	7.3	0.4	5.8	2.3	0.0	0.0	0.0	3.4	0.0	36.3
I	142.3	70.6	4.9	2.6	15.9	64.4	30.6	0.3	15.9	0.0	1.9	0.0	6.9	1.4
J	0.0	1.3	0.0	0.0	0.0	0.0	0.0	1.2	0.0	0.0	0.0	0.0	0.0	0.6
K	3.1	0.1	0.0	0.0	0.0	2.4	0.0	0.2	0.1	0.1	0.0	0.0	0.0	6.8
L	0.4	18.1	1.0	0.0	0.2	11.1	9.2	9.2	2.3	0.5	0.0	24.6	0.0	67.9
M	0.3	20.3	25.2	0.0	0.0	12.9	0.0	8.9	0.6	0.0	0.0	0.5	0.0	32.3
N	4.0	21.2	0.1	0.1	0.7	37.5	83.0	3.6	6.5	0.0	0.0	6.1	0.0	151.5
O	12.1	9.1	23.1	0.0	88.7	14.6	28.3	45.1	8.3	17.6	0.3	0.5	0.0	64.3
P	0.0	20.3	9.7	0.0	46.9	2.2	6.3	4.9	0.0	0.0	0.0	0.3	0.0	6.4
Q	0.0	0.0	0.0	0.0	0.0	0.0	0.0	14.8	0.0	0.0	0.0	0.0	0.0	1.0
R	5.7	62.1	2.1	0.0	5.9	21.5	20.3	11.9	5.6	0.3	0.0	10.7	0.0	94.0
S	0.5	23.6	7.4	0.1	0.1	43.7	77.9	30.7	0.0	2.6	0.0	21.1	0.0	257.8
T	0.7	60.4	0.5	0.0	31.9	38.3	4.4	14.3	0.0	10.9	0.0	34.2	0.2	137.7
U	18.6	0.5	6.0	0.0	53.7	43.9	16.9	0.0	0.0	0.0	0.1	0.1	0.1	13.3
V	0.0	2.8	0.0	0.0	0.0	0.5	0.0	0.4	0.0	0.0	0.0	0.0	0.0	0.1
W	3.4	10.4	0.0	0.0	1.6	2.8	0.0	0.0	0.0	0.0	0.0	0.0	0.0	10.2
X	0.0	0.1	16.5	0.0	0.0	0.0	2.1	0.0	0.0	0.0	0.0	0.0	0.0	3.6
Y	0.6	15.5	5.0	0.0	0.2	25.2	0.3	0.1	0.0	0.1	0.0	0.0	0.9	96.1
Z	0.0	0.2	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.1	0.0
SP	27.4	135.2	71.6	4.8	53.2	136.3	251.9	30.0	15.7	54.7	0.5	16.6	0.1	0.0

Transposition Ciphers (contd.)

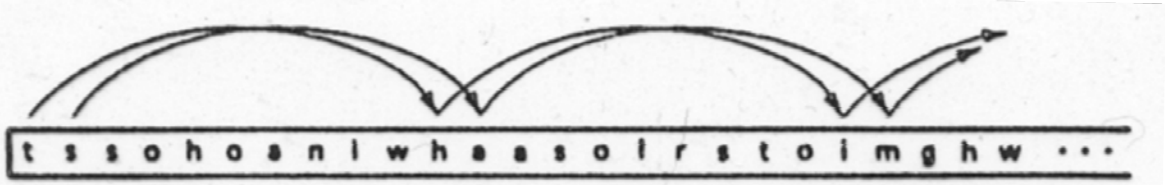


Figure 2-8 Positions of Adjacent Letters in Ciphertext

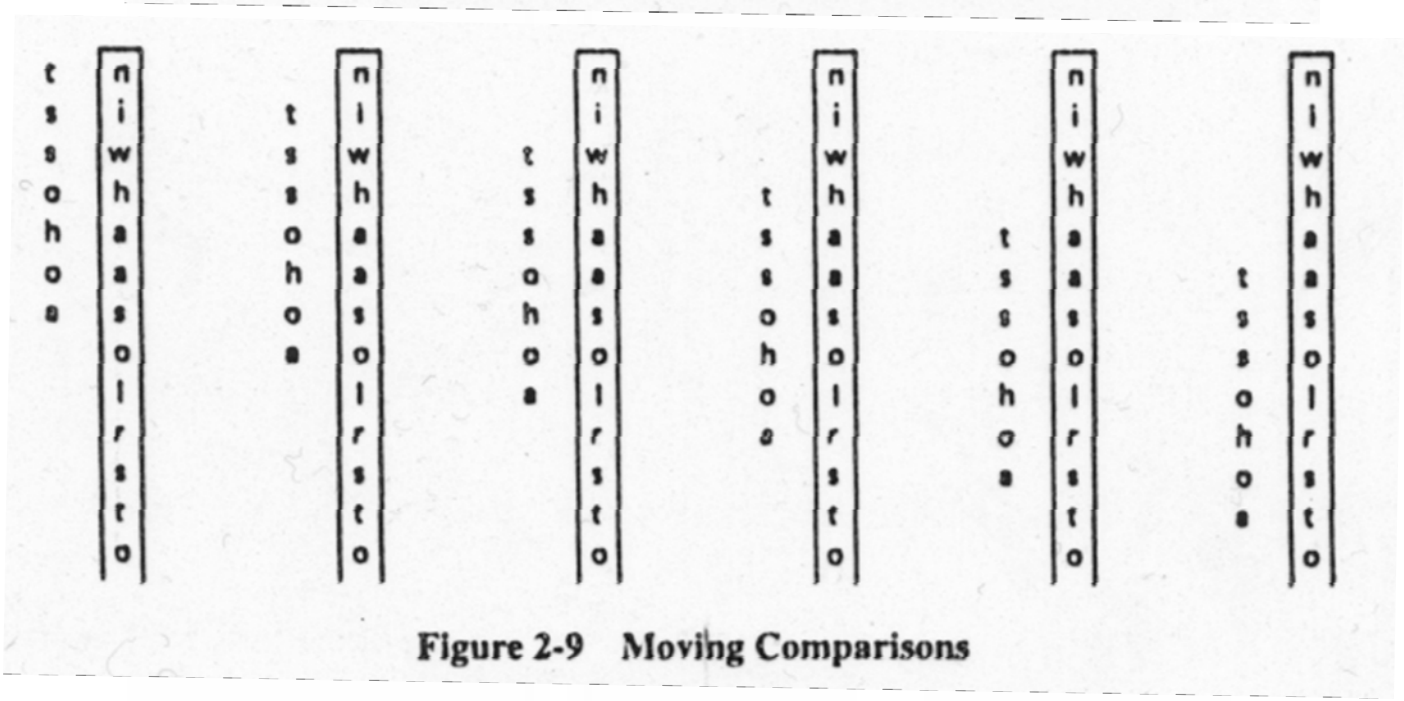


Figure 2-9 Moving Comparisons

Transposition Ciphers (contd.)

Double Columnar Transposition

- Example ($c_1 = 10$; $c_2 = 15$)
- Ciphertext (First Transposition)

```
T S H O H H A O S E I G W I R
S E A T W I T T I O S O R O R
A S A N K M H N C S E O S I X
S W P P X E A O X Y Q S R D X
```

- Ciphertext (Second Transposition)

```
TSASS ESWHA APOTN PHWKX HIMEA THAOT NOSIC
XEOSY ISEQG OOSWR SRIOI DRRXX
```

Transposition Ciphers (contd.)

```
tssoh oaniw haaso lrsto imghw
utpir seeoa mrook istwc nasns
tssoh oaniw haaso lrsto (i(m(g(h(w
(u(t(p(i(r s)e)e)o)a) m)r)o)o)k) istwc nasns
```

Table 2-10 Single Columnar Transposition

T	H	(I	S)	I
S	A	(M	E)	S
S	A	(G	E)	T
O	S	(H	O)	W
H	O	(W	A)	C
O	L	(U	M)	N
A	R	(T	R)	A
N	S	(P	O)	S
I	T	(I	O)	N
W	O	(R	K)	S

Table 2-11 Second Columnar Pattern

T	S	S	O	H	O	A
N	I	W	H	A	A	S
O	L	R	S	T	O	(I
(M	(G	(H	(W	(U	(T	(P
(I	(R	S)	E)	E)	O)	A)
M)	R)	O)	O)	K)	I	S
T	W	C	N	A	S	N
S	X	X	X	X	X	X

```
tno(m(i m)tssi l(g(rr)w xswr(h s)o)cxo
hs(we)o) nxhat (ue)k)ax oao(to) isxas (i(pa)sn x
```

Transposition Ciphers (contd.)

Breaking Double Transposition Ciphers

- Relationship between plaintext/ciphertext characters
- $p_i = c^1_{r_1 \cdot ([(i-1) \bmod c_1] + (i-1)/c_1 + 1)}$
- $c^1_i = c^2_{r_2 \cdot ([(i-1) \bmod c_2] + (i-1)/c_2 + 1)}$
- Use digrams and trigrams to compute parameters (c_1, r_1, c_2, r_2)

Product Ciphers

- Combine two or more approaches to strengthen encryption
- $E_1 = \{ P \}_{K_1}$
- $E_2 = \{ E_1 \}_{K_2} = \{ \{ P \}_{K_1} \}_{K_2}$

Fractionated Morse

FRACTIONATED MORSE

Table 2-12 Morse Code

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

F	R	A	C	T	I	O	N	A
..-.	.-.	.-	-.-.	-	..	---	-.	.-
T	**E**	**D**		**M**	**O**	**R**	**S**	**E**
-	.	-..		--	---	.-.	...	.

or

..-.|.-.|.-|-.-.|-|..|---|-.|.-|-|.|-..||--|---|.-.|...|.

(Note that a break between words is shown as | |, or a long pause.)

Fractionated Morse (contd.)

Example

As shown previously, the message

FRACTIONATED MORSE

is represented in Morse code as

```
..-.|.-.|.-|-.-.|-|..---|-.|.-|
-|.|-..||--|---|.-.|...|.
```

We begin fractionated Morse by breaking this message into blocks of three symbols. If the last block does not have three symbols, we fill it with the separator *l*.

```
..- .|. -.| .-| -.- .|- |.. |-- -|- .|.
-|- |.| -.. ||- -|- --| .-. |.. .|.
```

The encryption is completed by replacing each block of three symbols by its letter equivalent from Table 2.13.

```
..-  .|.  -.|  .-|  -.-  .|-  |..  |--  -|-  .|.
 o    l    d    f    c    a    p    t    k    l

-|-  |.|  -..  ||-  -|-  --|  .-.  |..  .|.
 k    r    b    z    k    i    e    p    l
```

Fractionated Morse (contd.)

Table 2-13 English Letters Associated with Morse Code Symbols

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

The final transmitted message is

oldfcaptklkrbzkiepl

Shannon Characteristics

Characteristics of "Good Ciphers" (1949)

- Amount of secrecy needed should determine the amount of effort needed for encryption and decryption (Principle of Timeliness)
- Keys and enciphering algorithm should be free from complexity
- Implementation should be as simple as possible
- Errors should not propagate and corrupt message
- Ciphertext Size ≤ Plaintext Size

CSEC
CYBER SECURITY EDUCATION CONSORTIUM

Trustworthy Encryption Systems

- Based on sound mathematics
- Analyzed by competent experts who have found it to be sound
- Stood the "test of time"
- Examples
  - DES (1977)
  - RSA (1978)
  - AES (2001)

NSF

ADVANCED TECHNOLOGICAL EDUCATION

Confusion vs. Diffusion

Confusion

- Interceptor should not be able to predict effect on ciphertext by changing one character of plaintext
  - Complex functional relationship between key/plaintext pair and ciphertext

Diffusion

- Changing plaintext affects many parts of the ciphertext
  - Information about a single plaintext character is distributed throughout the ciphertext

Stream vs. Block Ciphers

Stream Ciphers (Convert $p_i \rightarrow c_i$)

- Substitution Ciphers
  - High Speed of Transformation
  - Low Error Propagation
  - Low Diffusion
  - Susceptibility to Malicious Insertions

Block Ciphers (Convert $P \rightarrow C$)

- Transposition Ciphers
  - Low Speed of Transformation
  - High Error Propagation
  - High Diffusion
  - Immunity to Malicious Insertions

CSEC
CYBER SECURITY EDUCATION CONSORTIUM

Breaking Encryption

Cryptanalysis

- Ciphertext Only Attack (only cipher text is known)
- Known Plaintext Attack (full plaintext is known)
- Probable Plaintext Attack (some plaintext is known)
- Chosen Plaintext Attack (sender's process is known)
- Chosen Ciphertext Attack (algorithm and ciphertext are known)

NSF

ADVANCED TECHNOLOGICAL EDUCATION