Name: Watcharapol Yotadee

Nickname: Fluke

Assignment Week 3

Cryptography

Here are three simple data encryption methods with examples:

a. *Caesar Cipher*
   - *Method: Shifts each letter in the plaintext by a fixed number of positions in the alphabet.*

     Example:
     Plaintext: "HELLO"
     Shift: 3
     H -> K
     E -> H
     L -> O
     L -> O
     O -> R
     Ciphertext: "KHOOR"

b. *Substitution Cipher*
   - *Method: Replaces each letter in the plaintext with another letter or symbol.*

     Example:
     Plaintext: "HELLO"
     Substitution Table:
     A -> Z
     B -> Y
     C -> X
     ...
     X -> C
     Y -> B
     Z -> A
     Ciphertext: "HVVDP"

c. *Transposition Cipher*
   - *Method: Rearranges the order of the letters in the plaintext.*

     Example:
     Plaintext: "HELLO WORLD"
     Key: 3 (every 3 letters)
     Ciphertext: "HLOEL DLWOR"

Name: Watcharapol Yotadee

Nickname: Fluke

Individual Assignment Week 3

1. Convert readable data (plaintext) into unreadable format (ciphertext) to prevent unauthorized people from understanding the meaning of the data. Using the simple data encoding methods.

   Plaintext:

   While these methods are simple to understand and implement
   They are not secure for protecting sensitive data

   a. Caesar Cipher

   Shift: 5 (English Letter)

   Plaintext: "While"
   Shift: 5
   W -> B
   h -> m
   i -> n
   l -> q
   e -> j
   Ciphertext: "Bmnqj"

   Plaintext: "these"
   Shift: 5
   t -> y
   h -> m
   e -> j
   s -> x
   e -> j
   Ciphertext: "ymjxj"

   Plaintext: "methods"
   Shift: 5
   m -> r
   e -> j
   t -> y
   h -> m
   o -> t
   d -> i
   s -> x
   Ciphertext: "rjymtix"

   Plaintext: "are"
   Shift: 5
   a -> f
   r -> w
   e -> j
   Ciphertext: "fwj"

Name: Watcharapol Yotadee

Nickname: Fluke

Plaintext: "simple"
Shift: 5
s -> x
i -> n
m -> r
p -> u
l -> q
e -> j
Ciphertext: "xnruqj"

Plaintext: "to"
Shift: 5
t -> y
o -> t
Ciphertext: "yt"

Plaintext: "understand"
Shift: 5
u -> z
n -> s
d -> i
e -> j
r -> w
s -> x
t -> y
a -> f
n -> s
d -> i
Ciphertext: "zsijwxyfsi"

Plaintext: "and"
Shift: 5
a -> f
n -> s
d -> i
Ciphertext: "fsi"

Name: Watcharapol Yotadee

Nickname: Fluke

Plaintext: "implement"
Shift: 5
i -> n
m -> r
p -> u
l -> q
e -> j
m -> r
e -> j
n -> s
t -> y
Ciphertext: "nruqjrjsy"

Plaintext: "They"
Shift: 5
T -> Y
h -> m
e -> j
y -> d
Ciphertext: "Ymjd"

Plaintext: "are"
Shift: 5
a -> f
r -> w
e -> j
Ciphertext: "fwj"

Plaintext: "not"
Shift: 5
n -> s
o -> t
t -> y
Ciphertext: "sty"

Plaintext: "secure"
Shift: 5
s -> x
e -> j
c -> h
u -> z
r -> w
e -> j
Ciphertext: "xjhzwj"

Name: Watcharapol Yotadee

Nickname: Fluke

Plaintext: "for"
Shift: 5
f -> k
o -> t
r -> w
Ciphertext: "ktw"

Plaintext: "protecting"
Shift: 5
p -> u
r -> w
o -> t
t -> y
e -> j
c -> h
t -> y
i -> n
n -> s
g -> l
Ciphertext: "uwtyjhynsl"

Plaintext: "sensitive"
Shift: 5
s -> x
e -> j
n -> s
s -> x
i -> n
t -> y
i -> n
v -> a
e -> j
Ciphertext: "xjsxnynaj"

Plaintext: "data"
Shift: 5
d -> i
a -> f
t -> y
a -> f
Ciphertext: "ifyf"

Name: Watcharapol Yotadee

Nickname: Fluke

b. Substitution Cipher

Plaintext:

While these methods are simple to understand and implement
They are not secure for protecting sensitive data

Substitution Table:

Normal letter	A	B	C	D	E	F	G	H	I	J	K	L
Substitution letter	*0*	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*A*	*B*

Normal letter	M	N	O	P	Q	R	S	T	U	V	W	X
Substitution letter	*C*	*D*	*E*	*F*	*G*	*H*	*I*	*J*	*K*	*L*	*M*	*N*

Normal letter	Y	Z	0	1	2	3	4	5	6	7	8	9
Substitution letter	*O*	*P*	*Q*	*R*	*S*	*T*	*U*	*V*	*W*	*X*	*Y*	*Z*

Ciphertext: *M78B4 J74I4 C4J7E3I 0H4 I8CFB4 JE KD34HIJ0D3 0D3 8CFB4C4DJ J74O 0H4 DEJ I42KH4 5EH FHEJ42J8D6 I4DI8J8L4 30J0*

2. Convert the following unreadable format message (ciphertext) to readable data (plaintext).

Using Method: "Transposition Cipher"

Key: Convert column to row then Rearranges to single line

Ciphertext:

M	n	p	a		r	s	e		R	r	e	h	o		r	T	i	p	n	s	t		e	n		
o		t	p	a	i			a	S	o			n	s	i	h	r	e		u		c	c	s	w	w
d	c	o	h	l	t	l	A	n	A	v	m	s	g	e	t	e	s	r	t	b	t	o	t	w	i	i
e	r	g	i	g	h	i	E	d		i	u	t	e	c	y		t	s	o	m	h	r		e	l	n
r	y	r	c	o	m	k	S		p	d	c	r	r	u	.	f		o		i	e	r	a	r	l	.

Plaintext:

"Modern cryptographic algorithms like AES and RSA provide much stronger security. The first person to submit the correct answer will win."