COURSE TECHNOLOGY
CENGAGE Learning™

Using Encryption

Lecture 7

Yet it may roundly be asserted that human ingenuity cannot concoct a cipher which human ingenuity cannot resolve.

EDGAR ALLAN POE, THE GOLD BUG

Learning Objectives

- Upon completion of this material, you should be able to:
  - Chronicle the most significant events and discoveries in the history of cryptology
  - Explain the basic principles of cryptography
  - Describe the operating principles of the most popular cryptographic tools
  - List and explicate the major protocols used for secure communications
  - Discuss the nature and execution of the dominant methods of attack used against cryptosystems

Introduction

- Cryptology: science of encryption; combines cryptography and cryptanalysis
- Cryptography: process of making and using codes to secure transmission of information
- Cryptanalysis: process of obtaining original message from encrypted message without knowing algorithms
- Encryption: converting original message into a form unreadable by unauthorized individuals
- Decryption: the process of converting the ciphertext message back into plaintext

Foundations of Cryptology

- Cryptology has a long and multicultural history
- With emergence of technology, need for encryption in information technology environment greatly increased
- All popular Web browsers use built-in encryption features for secure e-commerce applications

Cipher Methods

- Plaintext can be encrypted through bit stream or block cipher method
- Bit stream: each plaintext bit transformed into cipher bit one bit at a time. Eg. XOR
- Block cipher: message divided into blocks (e.g., sets of 8- or 16-bit blocks) and each is transformed into encrypted block of cipher bits using algorithm and key. Eg. substitution, transposition, XOR or combinations of these operations.

Substitution Cipher

- Substitute one value for another
- Monoalphabetic substitution: uses only one alphabet
- Polyalphabetic substitution: more advanced; uses two or more alphabets
- Vigenère cipher: advanced cipher type that uses simple polyalphabetic code; made up of 26 distinct cipher alphabets

Monoalphabetic substitution

- A three-character substitution to the right results in the following transformation of the standard English alphabet:
- Initial alphabet yields
  ABCDEFGHIJKLMNOPQRSTUVWXYZ
- Encryption alphabet
  DEFGHIJKLMNOPQRSTUVWXYZABC
- Within this substitution scheme, the plaintext MOM would be encrypted into the ciphertext PRP.

Polyalphabetic substitution

- Plaintext
- ABCDEFGHIJKLMNOPQRSTUVWXYZ
- Substitution cipher 1
  DEFGHIJKLMNOPQRSTUVWXYZABC
- Substitution cipher 2
  GHIJKLMNOPQRSTUVWXYZABCDEF
- Substitution cipher 3
  JKLMNOPQRSTUVWXYZABCDEFGHI
- Substitution cipher 4
  MNOPQRSTUVWXYZABCDEFGHIJKL
- TEXT = WKGF

Vigenere Cipher

- You could perform an encryption by simply starting in the first row and finding a substitute for the first letter of plaintext, and then moving down the rows for each subsequent letter of plaintext.
- With this method, the word SECURITY in plaintext becomes ---------- in ciphertext.

Vigenere Cipher

- A much more sophisticated way to use the Vigenère square is to use a keyword to represent the shift.
- To accomplish this, you begin by writing a keyword above the plaintext message.
- For example, suppose the plaintext message was “SACK GAUL SPARE NO ONE” and the keyword was ITALY. We thus end up with the following:

```
ITALYITALYITALYITA
SACKGAULSPARENOONE
```

	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
1	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
2	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
3	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
4	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
5	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
6	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
7	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
8	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
9	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
10	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
11	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
12	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
13	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
14	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
15	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
16	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
17	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
18	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
19	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
20	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
21	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
22	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
23	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
24	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
25	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
26	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

Table 8-2 The Vigenère Square

Transposition Cipher

- Easy to understand, but if properly used, produces ciphertext that is difficult to decipher
- Rearranges values within a block to create ciphertext
- Can be done at the bit level or at the byte (character) level
- To make the encryption even stronger, the keys and block sizes can be made much larger

Transposition Cipher

- Plaintext message
- 00100101011010111001010101010100
- Key pattern
- 1→4, 2 →8, 3→1, 4→ 5, 5 →7, 6 →2, 7 →6, 8 →3
- Bit locations:
- 87654321 87654321 87654321 87654321
- Plaintext 8-bit blocks:
  00100101|01101011|10010101|01010100
- Ciphertext:
  00001011|10111010|01001101|01100001

Transposition Cipher

Letter locations:	87654321	87654321	87654321	87654321
Plaintext:	SACKGAUL	SPARENOO	NE	
Key: Same key as above, but characters transposed, not bits.				
Ciphertext:	UKAGLSCA	ORPEOSAN	E N	

Exclusive OR (XOR)

- Function of Boolean algebra; two bits are compared
  - If two bits are identical, result is binary 0
  - If two bits not identical, result is binary 1
- A very simple symmetric cipher that is used in many applications where security is not a defined requirement

First Bit	Second Bit	Result
0	0	0
0	1	1
1	0	1
1	1	0

Table 8-3 XOR Truth Table

Vernam Cipher

- Developed at AT&T
- Uses set of characters once per encryption process
- To perform:
  - The pad values are added to numeric values that represent the plaintext that needs to be encrypted
  - Each character of the plaintext is turned into a number and a pad value for that position is added
  - The resulting sum for that character is then converted back to a ciphertext letter for transmission
  - If the sum of the two values exceeds 26, then 26 is subtracted from the total

Vernam Cipher

Plaintext:	S	A	C	K	G	A	U	L	S	P	A	R	E	N	O	O	N	E
Plaintext value:	19	01	03	11	07	01	21	12	19	16	01	18	05	14	15	15	14	05
One-time pad text:	F	P	Q	R	N	S	B	I	E	H	T	Z	L	A	C	D	G	J
One time pad value:	06	16	17	18	14	19	02	09	05	08	20	26	12	01	03	04	07	10
Sum of plaintext and pad:	25	17	20	29	21	20	23	21	24	24	21	44	17	15	18	19	21	15
After modulo Subtraction:				03								18						
Ciphertext:	Y	Q	T	C	U	T	W	U	X	X	U	R	Q	O	R	S	U	O

Book or Running Key Cipher

- Uses text in book as key to decrypt a message
- Ciphertext contains codes representing page, line, and word numbers
- Algorithm is the mechanical process of:
  - Looking up the references from the ciphertext
  - Converting each reference to a word by using the ciphertext's value and the key
- Typical sources are dictionaries and thesauruses
- Eg. 259,19,8; 22,3,8; 375,7,4; 394,17,2.