

Cryptography and Network Security Intro., Conventional

Xiang-Yang Li

CS595-Cryptography and Network Security

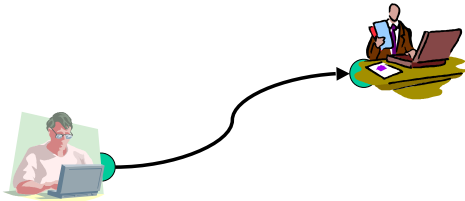
Introduction

The art of war teaches us not on the likelihood of the enemy's not coming, but on our own readiness to receive him; not on the chance of his not attacking, but rather on the fact that we have made our position unassailable.

--The art of War, Sun Tzu

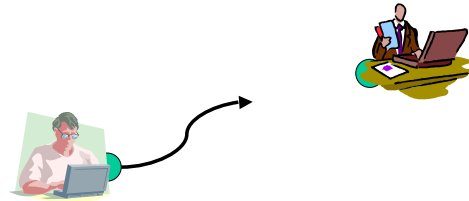
CS595-Cryptography and Network Security

Information Transferring



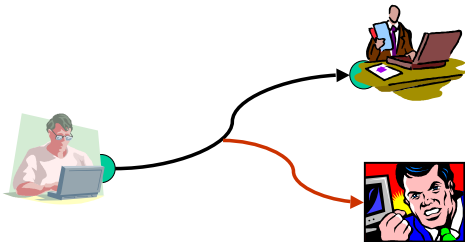
CS595-Cryptography and Network Security

Attack: Interruption



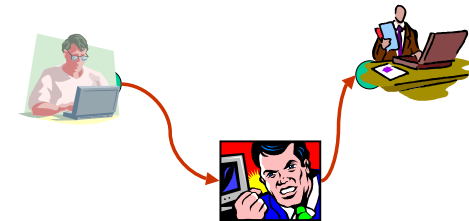
CS595-Cryptography and Network Security

Attack: Interception



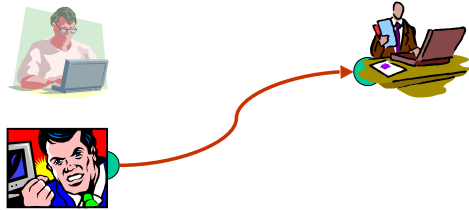
CS595-Cryptography and Network Security

Attack: Modification



CS595-Cryptography and Network Security

Attack: Fabrication



CS595-Cryptography and Network Security

Attacks, Services and Mechanisms

- ❑ Security Attacks
 - Action compromises the information security
- ❑ Security Services
 - Enhances the security of data processing and transferring
- ❑ Security mechanism
 - Detect, prevent and recover from a security attack

CS595-Cryptography and Network Security

Important Features of Security

- ❑ Confidentiality, authentication, integrity, non-repudiation, non-deny, availability, identification,

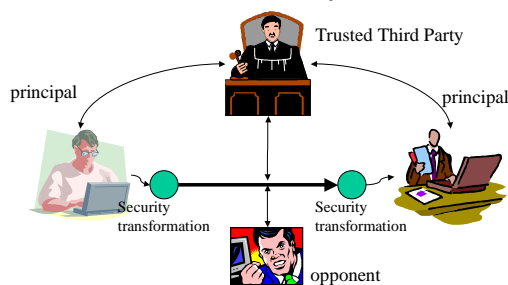
CS595-Cryptography and Network Security

Attacks

- ❑ Passive attacks
 - Interception
 - Release of message contents
 - Traffic analysis
- ❑ Active attacks
 - Interruption, modification, fabrication
 - Masquerade
 - Replay
 - Modification
 - Denial of service

CS595-Cryptography and Network Security

Network Security Model



CS595-Cryptography and Network Security

Cryptography

- ❑ Cryptography is the study of
 - **Secret** (crypto-) **writing** (-graphy)
- ❑ Concerned with developing algorithms:
 - Conceal the context of some message from all except the sender and recipient (privacy or secrecy), and/or
 - Verify the correctness of a message to the recipient (**authentication**)
 - Form the basis of many technological solutions to computer and communications security problems

CS595-Cryptography and Network Security

Basic Concepts

- ❑ **Cryptography**
 - The art or science encompassing the principles and methods of transforming an intelligible message into one that is unintelligible, and then retransforming that message back to its original form
- ❑ **Plaintext**
 - The original intelligible message
- ❑ **Ciphertext**
 - The transformed message

CS595-Cryptography and Network Security

Basic Concepts

- ❑ **Cipher**
 - An algorithm for transforming an intelligible message into unintelligible by transposition and/or substitution
- ❑ **Key**
 - Some critical information used by the cipher, known only to the sender & receiver
- ❑ **Encipher** (encode)
 - The process of converting plaintext to ciphertext
- ❑ **Decipher** (decode)
 - The process of converting ciphertext back into plaintext

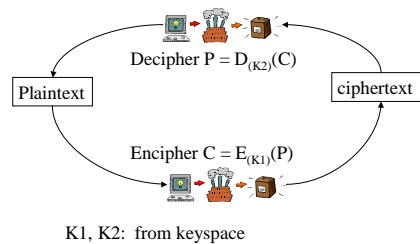
CS595-Cryptography and Network Security

Basic Concepts

- ❑ **Cryptanalysis**
 - The study of principles and methods of transforming an unintelligible message back into an intelligible message *without* knowledge of the key. Also called **codebreaking**
- ❑ **Cryptology**
 - Both cryptography and cryptanalysis
- ❑ **Code**
 - An algorithm for transforming an intelligible message into an unintelligible one using a code-book

CS595-Cryptography and Network Security

Encryption and Decryption



CS595-Cryptography and Network Security

Security

- ❑ Two fundamentally different security
 - **Unconditional security**
 - No matter how much computer power is available, the cipher cannot be broken
 - **Computational security**
 - Given limited computing resources (e.g. time needed for calculations is greater than age of universe), the cipher cannot be broken

CS595-Cryptography and Network Security

History

- ❑ **Ancient ciphers**
 - Have a history of at least 4000 years
 - Ancient Egyptians enciphered some of their hieroglyphic writing on monuments
 - Ancient Hebrews enciphered certain words in the scriptures
 - 2000 years ago Julius Caesar used a simple substitution cipher, now known as the Caesar cipher
 - Roger Bacon described several methods in 1200s

CS595-Cryptography and Network Security

History

- ❑ **Ancient ciphers**
 - Geoffrey Chaucer included several ciphers in his works
 - Leon Alberti devised a cipher wheel, and described the principles of frequency analysis in the 1460s
 - Blaise de Vigenère published a book on cryptology in 1585, & described the polyalphabetic substitution cipher
 - Increasing use, esp in diplomacy & war over centuries

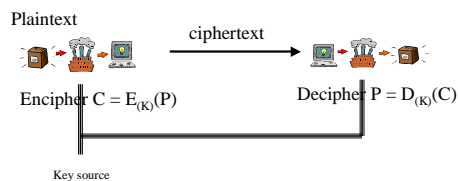
CS595-Cryptography and Network Security

Classical Cryptographic Techniques

- ❑ Two basic components of classical ciphers:
 - **Substitution:** letters are replaced by other letters
 - **Transposition:** letters are arranged in a different order
- ❑ These ciphers may be:
 - **Monoalphabetic:** only one substitution/ transposition is used, or
 - **Polyalphabetic:** where several substitutions/ transpositions are used
- ❑ **Product cipher:**
 - several ciphers concatenated together

CS595-Cryptography and Network Security

Encryption and Decryption



CS595-Cryptography and Network Security

Key Management

- ❑ Using secret channel
- ❑ Encrypt the key
- ❑ Third trusted party
- ❑ The sender and the receiver generate key
 - The key must be same

CS595-Cryptography and Network Security

Attacks

- ❑ Recover the message
- ❑ Recover the secret key
 - Thus also the message
- ❑ Thus the number of keys possible must be large!

CS595-Cryptography and Network Security

Possible Attacks

- ❑ Ciphertext only
 - Algorithm, ciphertext
- ❑ Known plaintext
 - Algorithm, ciphertext, plaintext-ciphertext pair
- ❑ Chosen plaintext
 - Algorithm, ciphertext, chosen plaintext and its ciphertext
- ❑ Chosen ciphertext
 - Algorithm, ciphertext, chosen ciphertext and its plaintext
- ❑ Chosen text
 - Algorithm, ciphertext, chosen plaintext and ciphertext

CS595-Cryptography and Network Security

Steganography

- ❑ Conceal the existence of message
 - Character marking
 - Invisible ink
 - Pin punctures
 - Typewriter correction ribbon
- ❑ Cryptography renders message unintelligible!

CS595-Cryptography and Network Security

Contemporary Equiv.

- ❑ Least significant bits of picture frames
 - 2048x3072 pixels with 24-bits RGB info
 - Able to hide 2.3M message
- ❑ Drawbacks
 - Large overhead
 - Virtually useless if system is known

CS595-Cryptography and Network Security

Caesar Cipher

- ❑ Replace each letter of message by a letter a fixed distance away (use the 3rd letter on)
- ❑ Reputedly used by Julius Caesar
- ❑ Example:

L FDPH L VDZ L FRQTXHUHG
I CAME I SAW I CONGUERED

- The mapping is

ABCDEFGHIJKLMNPOQRSTUVWXYZ
DEFGHIJKLMNPOQRSTUVWXYZABC

CS595-Cryptography and Network Security

Mathematical Model

- ❑ Description
 - Encryption $E_{(k)} : i \rightarrow i + k \text{ mod } 26$
 - Decryption $D_{(k)} : i \rightarrow i - k \text{ mod } 26$

CS595-Cryptography and Network Security

Cryptanalysis: Caesar Cipher

- ❑ Key space: 26
 - Exhaustive key search
- ❑ Example
 - GDUCUGQFRMPCNJYACJCRRCPO
HEVDVHRGSNQDOKZBBDKSSDQR
 - Plaintext:
JGXFJXTIUPSFMQMBDFMFUFSTKHYGYKUJVGRNCEGNG
VVGTV
 - Ciphertext:
LIZHZLVKWRUHSODFHOHWWHUVMJAIAMWXSIVITPEGI
PIXXIVW

CS595-Cryptography and Network Security

Character Frequencies

- ❑ In most languages letters are not equally common
 - in English e is by far the most common letter
- ❑ Have tables of single, double & triple letter frequencies
- ❑ Use these tables to compare with letter frequencies in ciphertext,
 - a monoalphabetic substitution does not change relative letter frequencies
 - do need a moderate amount of ciphertext (100+ letters)

CS595-Cryptography and Network Security

Letter Frequency Analysis

- ❑ Single Letter
 - A,B,C,D,E,.....
- ❑ Double Letter
 - TH,HE,IN,ER,RE,ON,AN,EN,....
- ❑ Triple Letter
 - THE,AND,TIO,ATI,FOR,THA,TER,RES,...

CS595-Cryptography and Network Security

Modular Arithmetic Cipher

- ❑ Use a more complex equation to calculate the ciphertext letter for each plaintext letter
- ❑ $E_{(a,b)} : i \rightarrow a*i + b \pmod{26}$
 - Need $\gcd(a,26) = 1$
 - Otherwise, not reversible
 - So, $a \neq 2, 13, 26$
 - Caesar cipher: $a=1$

CS595-Cryptography and Network Security

Cryptanalysis

- ❑ Key space: $23*26$
 - Brute force search
- ❑ Use letter frequency counts to guess a couple of possible letter mappings
 - frequency pattern not produced just by a shift
 - use these mappings to solve 2 simultaneous equations to derive above parameters

CS595-Cryptography and Network Security

Playfair Cipher

Used in WWI and WWII

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

Key: simple

CS595-Cryptography and Network Security

Playfair Cipher

- ❑ Use filler letter to separate repeated letters
- ❑ Encrypt two letters together
 - Same row— followed letters
 - ac--bd
 - Same column— letters under
 - qw--wi
 - Otherwise—square's corner at same row
 - ar--bq

CS595-Cryptography and Network Security

Analysis

- ❑ Size of diagrams: 25!
- ❑ Difficult using frequency analysis
 - But it still reveals the frequency information

CS595-Cryptography and Network Security

Hill Cipher

- ❑ Encryption
 - Assign each letter an index
 - $C=KP \text{ mod } 26$
 - Matrix K is the key
- ❑ Decryption
 - $P=K^{-1}C \text{ mod } 26$

CS595-Cryptography and Network Security

Analysis

- ❑ Difficult to use frequency analysis
- ❑ But vulnerable to known-plaintext attack

CS595-Cryptography and Network Security

Polyalphabetic Substitution

- ❑ Use more than one substitution alphabet
- ❑ Makes cryptanalysis harder
 - since have more alphabets to guess
 - and flattens frequency distribution
 - same plaintext letter gets replaced by several ciphertext letter, depending on which alphabet is used

CS595-Cryptography and Network Security

Vigenère Cipher

- ❑ Basically multiple Caesar ciphers
- ❑ key is multiple letters long
 - $K = k_1 k_2 \dots k_d$
 - i th letter specifies i th alphabet to use
 - use each alphabet in turn, repeating from start after d letters in message
- ❑ Plaintext THISPROCESSCANALSOBEEXPRESSED
Keyword CIPHERCIPHERCIPHERCIPHER
Ciphertext VPXZTIQKTZWTCVPSWDFDMTETIGAHLH

CS595-Cryptography and Network Security

One-time Pad

- ❑ Gilbert Vernam (AT&T)
- ❑ Encryption
 - $C=P\oplus K$
- ❑ Decryption
 - $P=C\oplus K$
- ❑ Difficulty: key K is as long as message P

CS595-Cryptography and Network Security

Transposition Methods

- ❑ Permutation of plaintext
- ❑ Example
 - Write in a square in row, then read in column order specified by the key
- ❑ Enhance: double or triple transposition
 - Can reapply the encryption on ciphertext

CS595-Cryptography and Network Security