NWEN 243

Networked Applications

Lecture 2: Introduction to Cryptography II

Lecturer: Aaron Chen
aaron.chen@ecs.vuw.ac.nz
463 5114
AM405

Computer Security Objectives

Confidentiality

- Data confidentiality
- Privacy

Integrity

- Data integrity
- System integrity

Availability

- Assures that systems work promptly and service is not denied to authorized users

Possible additional concepts

Authenticity

- Verifying that users are who they say they are and that each input arriving at the system came from a trusted source

Accountability

- The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity

Discussion …

- What security requirements do we need for the following?
  - A system that maintains student grade information.
  - A system that stores patient information in a hospital.
  - A public Web site for a university.

Security attacks

- A means of classifying security attacks, used both in X.800 and RFC 4949, is in terms of passive attacks and active attacks
- A passive attack attempts to learn or make use of information from the system but does not affect system resources
- An active attack attempts to alter system resources or affect their operation

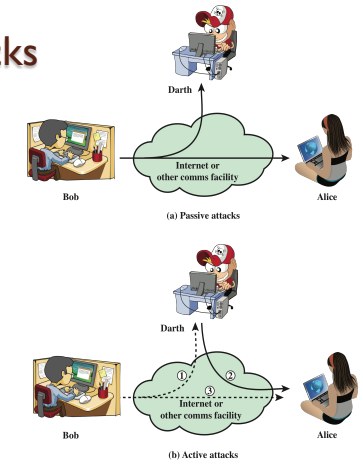
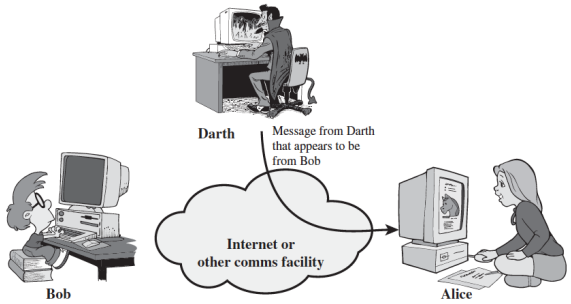


Figure 1.1 Security Attacks

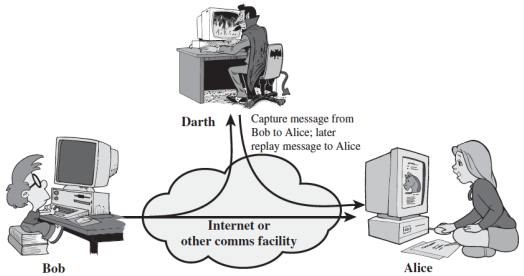
More on active attacks

- Masquerade



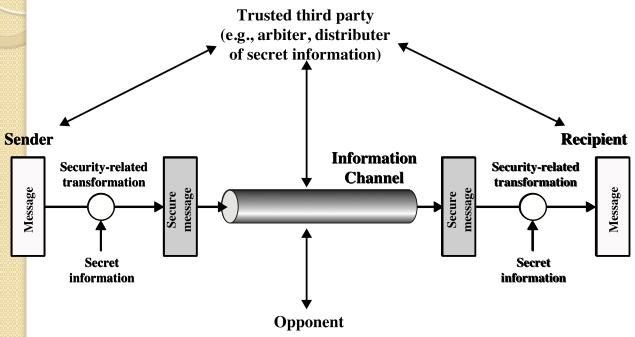
Other forms

- Replay attack



- Modification of messages
- Denial of service

Model for Network Security



Discussion …

- In view of the general model for network security, what algorithms are essential for building a network security system?

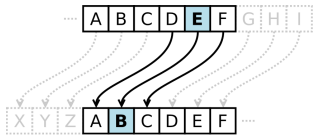
Some basic terminologies

- Plaintext - original message
- Ciphertext - coded message
- Cipher - algorithm for transforming plaintext to ciphertext
- Key - info used in cipher known only to sender/receiver
- Encipher (encrypt) - converting plaintext to ciphertext
- Decipher (decrypt) - recovering plaintext from ciphertext

- Cryptanalysis (code breaking) - study of principles/methods of deciphering ciphertext without knowing key

Reminder: Caesar Cypher I

- The Caesar cypher outlined last lecture is a shift cipher



- Using the cipher

```
Plaintext:
THE QUICK BROWN FOX JUMPS OVER THE LAZY
DOG
Ciphertext:
QEB NRFZH YOLTK CLU GRJMP LSBO QEB IXWV
ALD
```

Mathematics behind Caesar cipher

- Encryption

$$E_n(x) = (x + n) \mod 26$$

- Decryption

$$D_n(x) = (x - n) \mod 26$$

- Question: what is the possible number of values for n?

Reminder: Caesar Cypher II

- Caesar cypher can be improved through random substitution.
  - The Kama-Sutra pairs
- This will be Lab 1

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

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

alice, meet you at the park, bob

jwrls, xssh pzk jh hes bjfv, uzu

The first analyitical cryptanalysis

- However, in about 850AD, early during the Arab renaissance, Al-Kindī broke the substitution cypher.
  - Central to this was his observation that each letter appears with a charactistic frequency.
  - By counting the frequencies of each letter in the encoded text, Al-Kindī could assign each of the substituted letters a small set of probable matches.
  - These are then tried in the text and the adjacent letters are inferred by their unique *personality* (i.e. q is always followed by u, h often goes before e but rarely after e).
  - The key can then be reverse engineered using a limited search…
  - This is Part of Lab 2

Letter probabilities (ENGLISH)

A	.082	N	.067
B	.015	O	.075
C	.028	P	.019
D	.043	Q	.001
E	.127	R	.060
F	.022	S	.063
G	.020	T	.091
H	.061	U	.028
I	.070	V	.010
J	.002	W	.023
K	.008	X	.001
L	.040	Y	.020
M	.024	Z	.001

Common pairs	TH, EA, OF, TO, IN, IT, IS, BE, AS, AT, SO, WE, HE, BY, OR, ON, DO, IF, ME, MY, UP
Common repeated letters	SS, EE, TT, FF, LL, MM and OO
Common triplets	THE, EST, FOR, AND, HIS, ENT or THA

Frequency analysis – an example

- Cyphertext given

```
wkh sdvvzrug lv vhyhq grqw whoo dqbrqh
```

- Obtain letter frequencies

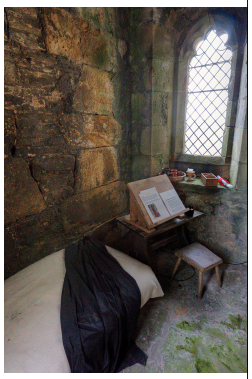
```
h = 5
v = 4
q = 3
r = 3
g = 3
d = 2
b = 1
k = 1
l = 1
s = 1
y = 1
```

The first Cryptanalysists

- When a secret is worth encrypting, it is certainly worth cracking by someone else.
  - Simple schemes such as the original Caeser Cypher and word subsitution were subject to analysis and decoding.
  - Artha-sastra, a book attributed to Kautilya, is an ancient Indian treatise on statecraft, economic policy and military strategy from 300BC. It recommended varieties of cryptanalysis, the process of breaking codes, to gain intelligence reports.
- However, the *substitution cypher* was considered unbreakable by many ancient scholars, and therefore guaranteed secure communication for almost a millennia.

While in Europe…

- Cyphers were used by monks for scribal amusement (some passages in the old testament were encrypted, such as the book of Jeremiah).
- The first European manual on cryptography, was by Franciscan monk Roger Bacon 1214-1294 AD.
- From about 1500 Cryptography and Cryptanalysis were becoming essential diplomatic tools, but…
- Cryptanalyists held the better hand.
- The problem was due to the monoalphabetic substitution on which we can perform freq analysis.



Return of the Cyptographers

- Leone Battista Alberti made the breakthough for constructing a better cypher in the 1460's.
- He proposed using two or *more* cypher alphabets (***polyalphabetic***) so that the substituion depended not only on the letter, but also its position.

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

j u l i s c a e r t v w x y z b d f g h k m n o p q **1**

l e o n b a t i s r u v w x y z c d f g h j k m p q **2**

alice, meet you at the fountain, bob

jvros, wsbh pzh jg hes azhygjsy, eze

le chiffre indéchiffrable

The Vigenère Cypher

1586

- Key selects alphabets
- text is then encrypted using the repeated key.

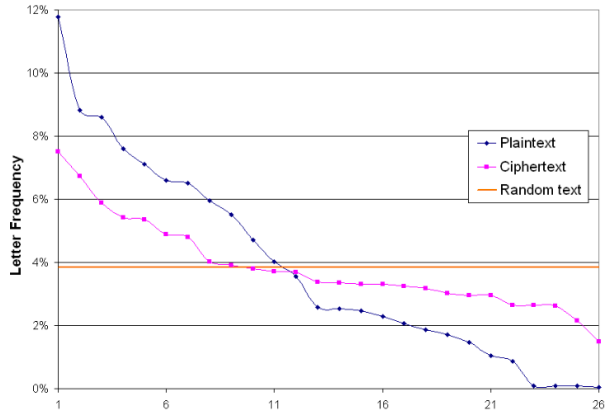
KEY: WHITE WHITE

TXT: what is life

CYP: SOIMMOSQMI

	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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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

Vulnerabilities of the Vigenère Cypher



Polyalphabetic Unwelcome

- Polyalphabetic cyphers where not used at the time, although considered 'practically' unbreakable -- as they were considered too difficult to use.
- Cryptographer's looked for a 'middle-ground' that would prevent frequency analysis:
  - Nomenclatures (Code words)
  - Homophones