# CS3200: Computer Networks

Lecture 33

IIT Palakkad

04 Nov, 2019

# Network Security

- For the first few decades of their existence, computer networks were primarily used by university researchers for sending email and by corporate employees for sharing printers.

- Security is a broad topic and covers a multitude of sins. In its simplest form, it is concerned with making sure that nosy people cannot read, or worse yet, secretly modify messages intended for other recipients.

- Network security problems can be divided roughly into four closely intertwined areas: secrecy, authentication, non-repudiation, and integrity control.

# Network Security

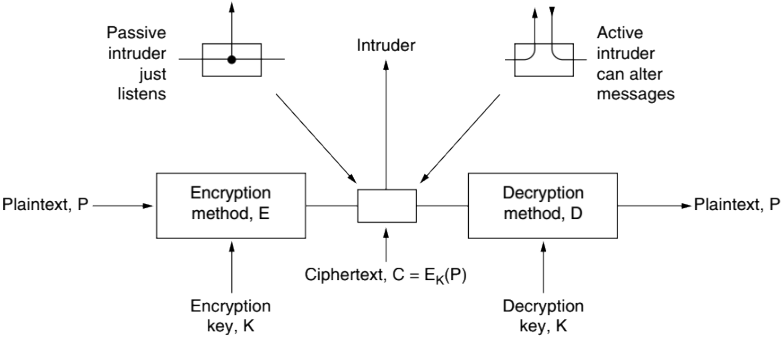
- **Secrecy**, also called confidentiality, has to do with keeping information out of the hands of unauthorized users.
- **Authentication** deals with determining whom you are talking to before revealing sensitive information.

repudiate means to reject.

- **Non-repudiation** deals with signatures: how do you prove that your customer really placed an electronic order? Or maybe he claims he never placed any order.
- **Integrity control** has to do with how you can be sure that a message you received was really the one sent and not something that a malicious adversary modified in transit or concocted.

# Cryptography

Cryptography comes from the Greek words for “secret writing.”



The art of breaking ciphers, known as **cryptanalysis**, and the art of devising them (cryptography) are collectively known as **cryptology**.

# Cryptanalysis

A cryptogram is a type of puzzle that consists of a short piece of encrypted text, encrypted using a ci

From the cryptanalyst's point of view, the cryptanalysis problem has three principal variations.

- When he has a quantity of ciphertext and no plaintext, he is confronted with the **ciphertext-only** problem

  eg: cryptograms in newspapers.

- When the cryptanalyst has some matched ciphertext and plaintext, the problem is called the **known plaintext** problem.

  i.e. I have a piece of plain text and its encryption too.

- Finally, when the cryptanalyst has the ability to encrypt pieces of plaintext of his own choosing, we have the **chosen plaintext** problem.

  Newspaper cryptograms could be broken trivially if the cryptanalyst were allowedto ask such questions as “What is the en

# Substitution Ciphers

- Each letter or group of letters is replaced by another letter or group of letters to disguise it.

- One of the oldest known ciphers is the **Caesar cipher**, attributed to Julius Caesar. With this method, $a$ becomes D, $b$ becomes E, $c$ becomes F, . . . , and $z$ becomes C.

- A slight generalization of the Caesar cipher allows the ciphertext alphabet to be shifted by $k$ letters, instead of always three.

- The next improvement is to have each of the symbols in the plaintext, say, the 26 letters for simplicity, map onto some other letter. For example,
  plaintext: 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
  ciphertext: Q W E R T Y U I O P A S D F G H J K L Z X C V B N M

# Breaking Substitution Ciphers

- Seems to be quiet secure. There are $26! \approx 4 \times 10^{26}$ possible keys.

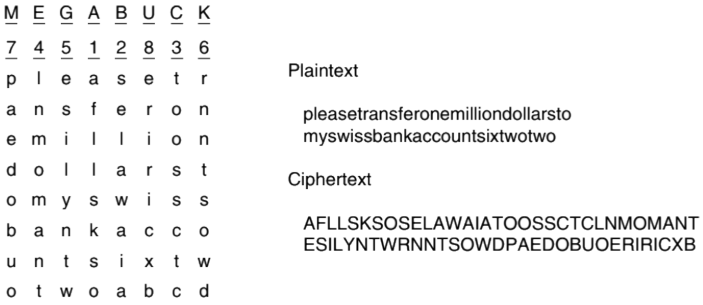
- Nevertheless, given a surprisingly small amount of ciphertext, the cipher can be broken easily.

- The basic attack takes advantage of the statistical properties of natural languages. In English, for example, *e* is the most common letter, followed by *t, o, a, n, i*, etc. The most common two-letter combinations, or **digrams**, are *th, in, er, re*, and *an*. The most common three-letter combinations, or **trigrams**, are *the, ing, and, and ion*.

# Transposition Ciphers

- Substitution ciphers preserve the order of the plaintext symbols but disguise them.

- **Transposition ciphers**, in contrast, reorder the letters but do not disguise them.



| M | E | G | A | B | U | C | K |
|---|---|---|---|---|---|---|---|
| 7 | 4 | 5 | 1 | 2 | 8 | 3 | 6 |
| p | l | e | a | s | e | t | r |
| a | n | s | f | e | r | o | n |
| e | m | i | l | l | i | o | n |
| d | o | l | l | a | r | s | t |
| o | m | y | s | w | i | s | s |
| b | a | n | k | a | c | c | o |
| u | n | t | s | i | x | t | w |
| o | t | w | o | a | b | c | d |

Plaintext

pleasetransferonemilliondollarsto
myswissbankaccountsixtwotwo

Ciphertext

AFLLSKSOSELAWAIATOOSSCTCLNMOMANT
ESILYNTWRNNTSOWDPAEDOBUOERIRICXB

# Breaking Transposition Ciphers

- By looking at the frequency of E, T, A, O, I, N, etc., it is easy to see if they fit the normal pattern for plaintext.
- The next step is to make a guess at the number of columns. In many cases, a probable word or phrase may be guessed at from the context.
- The remaining step is to order the columns. When the number of columns, $k$, is small, each of the $k(k-1)$ column pairs can be examined in turn to see if its digram frequencies match those for English plaintext.
- The pair with the best match is assumed to be correctly positioned. Now each of the remaining columns is tentatively tried as the successor to this pair. The column whose digram and trigram frequencies give the best match is tentatively assumed to be correct.