Lecture 2:

Classical Encryption Techniques I

4th Year- Course, CCSIT, UoA

Lecture Goals

1. To introduce the rudiments of encryption vocabulary.
2. To trace the history of some early approaches to cryptography.
3. To emphasize the basic principles of *substitution* and *transposition*, which are still valid till now (despite of the change of technology).

Vocabulary of Classical Encryption (1)

- **plaintext:** This is the original message that we want to encrypt
- **ciphertext**: The encrypted (message) output
- **enciphering or encryption**: The process by which plaintext is converted into ciphertext
- **encryption algorithm**: The sequence of data processing steps that go into transforming plaintext into ciphertext.
  - Various parameters used by an encryption algorithm are derived from a *secret key*.
  - In classical cryptography for commercial and other civilian applications, the encryption algorithm is made *public*.

Vocabulary of Classical Encryption (2)

- **secret key**: A secret key is used to set some or all of the various parameters used by the encryption algorithm. The important thing to note is that the same secret key is used for encryption and decryption in classical cryptography.
- **deciphering or decryption**: Recovering plaintext from ciphertext
- **decryption algorithm**: The sequence of data processing steps that go into transforming ciphertext back into plaintext.
  - Various parameters used by a decryption algorithm are derived from the same secret key that was used in the encryption algorithm.
  - In classical cryptography for commercial and other civilian applications, the decryption algorithm is made public.

Vocabulary of Classical Encryption (3)

- **cryptography**: The many schemes available today for encryption and decryption
- **cryptographic system**: Any single scheme for encryption
- **cipher:** A cipher means the same thing as a "cryptographic system"
- **block cipher**: A block cipher processes a block of input data at a time and produces a ciphertext block of the same size.
- **stream cipher**: A stream cipher encrypts data on the fly, usually one byte (or bit) at time.

Vocabulary of Classical Encryption (4)

- **cryptanalysis**: Means "breaking the code". Cryptanalysis relies on a knowledge of the encryption algorithm and some knowledge of the possible structure of the plaintext (such as the structure of a typical inter-bank financial transaction) for a partial or full reconstruction of the plaintext from ciphertext. Additionally, the goal is to also infer the key for decryption of future messages. The precise methods used for cryptanalysis depend on whether:

    1. the "attacker" has just a piece of ciphertext,
    2. or pairs of plaintext and ciphertext,
    3. how much structure is possessed by the plaintext,
    4. and how much of that structure is known to the attacker.

Vocabulary of Classical Encryption (5)

- **brute-force attack**: When encryption and decryption algorithms are publicly available, a brute-force attack means trying every possible key on a piece of ciphertext until an intelligible translation into plaintext is obtained.
- **key space**: The total number of all possible keys that can be used in a cryptographic system. For example, DES uses a 56-bit key. So the key space is of size 2^{56}, which is approximately the same as 7.2×10^{16}.
- **cryptology**: Cryptography and cryptanalysis together constitute the area of cryptology

Building Blocks of Classical Encryption Techniques

Two building blocks of all classical encryption techniques are substitution and transposition.

1. **Substitution** means replacing an element of the plaintext with an element of ciphertext.
2. **Transposition** means rearranging the order of appearance of the elements of the plaintext. Transposition is also referred to as *permutation*.

Caesar Cipher (1)

- This is the earliest known example of a substitution cipher.
- Each character of a message is replaced by a character ***three*** position down in the alphabet.

plaintext: a r e y o u r e a d y

ciphertext: DUH BRX UHDGB

Note that the alphabet is wrapped around, so that the letter following Z is A. We can define the transformation by listing all possibilities, as follows:

plain: 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

cipher: 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

Caesar Cipher (2)

- Let us assign a numerical equivalent to each letter:

a	b	c	d	e	f	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12

n	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25

- If we represent each letter of the alphabet by an integer that corresponds to its position in the alphabet, the formula for replacing each character 'p' of the plaintext with a character 'C' of the ciphertext can be expressed as

$$C = E(3, p) = (p + 3) \bmod 26$$

Caesar Cipher (3)

- A more general version of this cipher that allows for any degree of shift would be expressed by

$$C = E(k, p) = (p + k) \bmod 26$$

- The formula for decryption would be

$$p = D(k, C) = (C - k) \bmod 26$$

- In these formulas, *'k'* would be the secret key [1,…, 25]. The symbols *'E'* and *'D'* represent encryption and decryption.

❖ *We define* ***a mod n*** *to be the remainder when* ***a*** *is divided by* ***n****. For example, 11 mod 7 = 4.*

Caesar Cipher (4)

- If it is known that a given ciphertext is a Caesar cipher, then a brute-force cryptanalysis is easily performed: simply try all the **25** possible keys.
- Three important characteristics of this problem enabled us to use a **brute-force** cryptanalysis:

1. The encryption and decryption algorithms are known.
2. There are only 25 keys to try.
3. The language of the plaintext is known and easily recognizable.

Monoalphabetic Ciphers (1)

- With only 25 possible keys, the Caesar cipher is far from secure. A dramatic *increase in the key space* can be achieved by allowing an arbitrary substitution.
- *A **permutation*** of a finite set of elements S is an ordered sequence of all the elements of S , with each element appearing exactly once.
- For example, if S = {a, b, c}, there are six permutations of S: abc, acb, bac, bca, cab, cba
- In general, there are ***n!*** permutations of a set of ***n*** elements, because the first element can be chosen in one of n ways, the second in n - 1 ways, the third in n – 2 ways, and so on.

Monoalphabetic Ciphers (2)

- In a monoalphabetic cipher, our substitution characters are a random permutation of the 26 letters of the alphabet.
- The *key now is the sequence of substitution letters*. In other words, the key in this case is the actual random permutation of the alphabet used.
- Note that there are 26! permutations of the alphabet. That is a number larger than 4×10^{26}.
- Such an approach is referred to as a ***monoalphabetic*** substitution cipher, because a single cipher alphabet (mapping from plain alphabet to cipher alphabet) is used per message