Sheet #2

1. Define the following terms:

Plaintext: The original message.
Ciphertext: The coded message.
Cryptology: The field of both cryptography and cryptanalysis
Cryptography: Study of encryption principles/methods
Cryptanalysis: The study of principles/ methods of deciphering ciphertext without knowing the keys
Deciphering: recovering plaintext from ciphertext
Enciphering: Converting plaintext to ciphertext
Cipher: Algorithm for transforming plaintext to ciphertext.

2. Classify the encryption system according to:
   (a) Key
   - Hash functions: no key
   - Secret key cryptography: one key
   - Public key cryptography: two keys - public, private

   (b) Operation
   - Substitution
   - Transposition
   - Product

   (c) Mode of text processing
   - Block
   - Stream

3. In which security service we can use encryption? Explain how?
   - Authentication
   - Confidentiality

4. List and briefly define types of cryptanalytic attacks based on what is known to the attacker.

Type of Attack	Known to Cryptanalyst
Ciphertext only	• Encryption algorithm • Ciphertext
Known plaintext	• Encryption algorithm • Ciphertext • One or more plaintext-ciphertext pairs formed with the secret key
Chosen plaintext	• Encryption algorithm • Ciphertext • Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key
Chosen ciphertext	• Encryption algorithm • Ciphertext • Purported ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated

Type of Attack	Known to Cryptanalyst
	with the secret key
Chosen text	• Encryption algorithm • Ciphertext • Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key • Purported ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key

5. What is the difference between an unconditionally secure cipher and a computationally secure cipher?

Unconditional security
–No matter how much computer power is available, the cipher cannot be broken
–The ciphertext provides insufficient information to uniquely determine the corresponding plaintext
Computational security
–The cost of breaking the cipher exceeds the value of the encrypted information
–The time required to break the cipher exceeds the useful lifetime of the information

6. Why we don't use One-Time-Pad although it is the most secure encryption technique?

The one-time pad offers complete security but, in practice, has two fundamental difficulties:

1- There is the practical problem of making large quantities of random keys. Any heavily used system might require millions of random characters on a regular basis. Supplying truly random characters in this volume is a significant task.
2- Even more daunting is the problem of key distribution and protection. For every message to be sent, a key of equal length is needed by both sender and receiver. Thus, a mammoth key distribution problem exists.

Problems

1- According to your understanding of the encryption systems, what is the violation in the following symmetric encryption algorithm?

Input: Key, PlainText
Steps: Define CipherTextChar
foreach character CH in PlainText
CipherTextChar = (CH + 12) %26
Output CipherTextChar

Solution

- The cipher text doesn't depend on the value of the key and so the output of the encryption algorithm doesn't change if the key is changed.

2- Using One-Time-Pad, if the key is a stream of random numbers between 0 and 26. For example, if the key is 3 19 5 ..., then the first letter of plaintext is encrypted with a shift of 3 letters, the second with a shift of 19 letters, the third with a shift of 5 letters, and so on.

a- Encrypt the plaintext **"sendmoremoney"** with the key stream 9 0 1 7 23 15 21 14 11 11 2 8 9.

b- Using the ciphertext produced in part a, find a key so that the cipher text decrypts to the plaintext **"cashnotneeded"**.

Solution

(a)

P	S	e	n	d	m	o	r	e	m	o	n	e	y
K	9	0	1	7	23	15	21	14	11	11	2	8	9
C	B	E	O	K	J	D	M	S	X	Z	P	M	H

(b)

P	c	a	s	h	n	o	t	n	e	e	d	e	d
C	B	E	O	K	J	D	M	S	X	Z	P	M	H
K	25	4	22	3	22	15	19	5	19	21	24	8	4

3- Considering this c++ code,

```
int main() {
    char plnChar,CipherChar;
    while (true){
          cin>> plnChar;
                CipherChar = (char) ('A' + ((plnChar - 'a' +3)%26));
          cout<< CipherChar<<endl;
    }
           return 0;
}
```

a- What type of encryption is the implemented one?
b- Which type of text processing modes does the code use?

Solution

(a) The code implements **Ceaser Cipher**- Substitution
(b) The text processing mode is: **Stream**

Best Regards