Department of Electronics

Cryptography

Fall 2019

Hasan Mahmood

hasan@qau.edu.pk

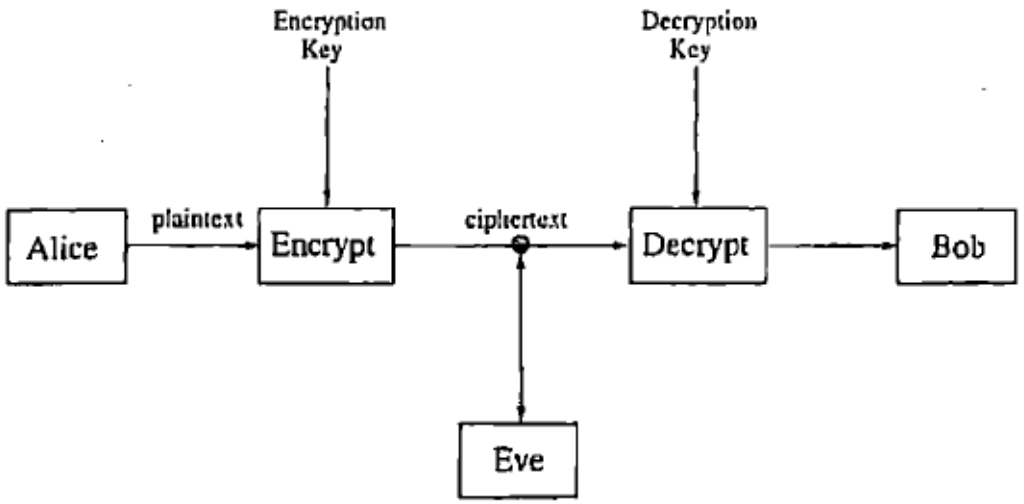
Week 1, 2 and 3

Introduction

- Keeping information secure
- Kings and generals communicated through encrypted methods
- Information ere, need more protection
- Electronics communications, Credit Cards, Bank Information, etc…
  - Cryptology: Study of communications over non-secure channels
  - Cryptography: Process of designing new systems
  - Cryptanalysis: Deals with the breaking of the secure systems
  - Coding: Compression, secrecy, **error correction**

Secure Communications

The basic communications scenario for cryptography



The role of the eavesdropper

- Alice and Bob want to communicate
- Eve/Oscar is the potential eavesdropper
- Encryption method is known to Eve
- Secret Key, protect the message

Attacks

The objectives of Eve?

1. Read the message.
2. Find the key and thus read all messages encrypted with that key.
3. Corrupt Alice's message into another message in such a way that Bob will think Alice sent the altered message.
4. Masquerade as Alice, and thus communicate with Bob even though Bob believes he is communicating with Alice.

Possible Attacks

1. Cipher text only: Eve has only the copy of the cipher text
2. Known Plain Text: Eve has the copy of the cipher text and the corresponding plain text
3. Chosen Plaintext: Eve gains temporary access to the encryption machine
4. Chosen Cipher text: Eve gains temporary access to the decryption machine

Kerckhoffs's Principle

- In assessing the security of a cryptosystem, one should always assume the enemy knows the method being used.
- Encryption Machines:
  - Captured
  - Defect
- Therefore, the security is based on the KEY

Symmetric and Public Key Algorithms

- Two Categories: Symmetric Key and Public Key
- Symmetric Key: The encryption and decryption keys are known to both Alice and Bob. The key is shared via secure method before the start of the communication.
- Encryption Key and Decryption Key are same
- Key exchange is a problem
- Solution: Public Key Cryptography.
- RSA, ELGamal system, NTRU (Lattice based), McEliece system (based on error correcting codes), etc.

Public Key Cryptography: Simple example

- Bob sends box and a lock to Alice
- Alice locks the message using Bob’s lock in the box
- Only Bob has the key to the lock used for the box
- Bob receives the locked box and opens with his own key
- Only Bob reads the message…

- Interception? Not suitable for large amount of data.
- Computationally complex to obtain secure key. 8-bit key?
- All information except the key is public. Useful method!

Symmetric Key Cryptography

- Two Types: Stream Ciphers and Block Ciphers
- Stream Ciphers: bits or bits of data as input
- Block Ciphers: block of input bits is used
- Most of the communications is accomplished in packets/frames, we will emphasize of block ciphers.

Codes and Ciphers

- Codes:
  - Combination of characters are replaced code words

- **Ciphers:**
  - Does not use the linguistic structure. Encrypts a string of charters

Key Length

- Security of a cryptographic algorithm is difficult to measure
- Most algorithms use Keys
- Strength depends on how difficult it is to find the key
- Brute force attack: Try every possible key! (Key length is important)
- 10^30 takes 3x10^1 years, longer than the predicted life of the universe
- Longer key plus the algorithm in combination are important
- (please refer to section 1.1.3 of the textbook for more details)

Cryptographic Applications I

1. **Confidentiality:** Eve should not be able to read Alice's message to Bob. The main tools are encryption and decryption algorithms.

2. **Data integrity:** Bob wants to be sure that Alice's message has not been altered. For example, transmission errors might occur. Also, an adversary might intercept the transmission and alter it before it reaches the intended recipient. Many cryptographic primitives, such as hash functions, provide methods to detect data manipulation by malicious or accidental adversaries.

Cryptographic Applications II

3. **Authentication:** Bob wants to be sure that only Alice could have sent the message he received. Under this heading, we also include identification schemes and password protocols (in which case, Bob is the computer). There are actually two types of authentication that arise in cryptography: entity authentication and data-origin authentication. Often the term *identification* is used to specify entity authentication, which is concerned with proving the identity of the parties involved in a communication. Data-origin authentication focuses on tying the information about the origin of the data, such as the creator and time of creation, with the data.

4. **Non-repudiation:** Alice cannot claim she did not send the message. Non-repudiation is particularly important in electronic commerce applications, where it is important that a consumer cannot deny the authorization of a purchase.

Applications

- **Digital Signatures**
  - The protocols that allow for electronic messages to be signed in such a way that everyone believes that the signer was the person who signed the document, and such that the signer cannot den signing the document
- **Identification**
  - Proving identity without reveling the password
- **Key establishment**
  - Protocol that provides authentication and security in key exchange between users on a network
- **Secret sharing**
  - Safe keeping, opening sage by multiple people
- **Security protocols**
  - Secure transactions over Internet, banking, credit cards
- **Electronic cash**
  - Electronic cash system that provides anonymity but catches the counterfeiters
- **Games**
  - Exchanging game information across rooms

Classical Cryptosystems: Shift Ciphers

- Older cryptosystems, used before advent of computers
- Shift Ciphers (originally used by Julius Caesar)

- **Plaintext:** *gaul is divided into three parts*

- **Ciphertext: (add 3 to each letter),** *x=x+k mod 26*

JDXOLVGLYLGHGLQWRWKUHHSDUWV.

- *Attacks: Ciphertext only, Known plaintext, Chosen plaintext, Chosen ciphertext*

Classical Cryptosystems: Affine Ciphers

The shift ciphers may be generalized and slightly strengthened as follows. Choose two integers α and β, with $\gcd(\alpha, 26) = 1$, and consider the function (called an *affine function*)

$$x \mapsto \alpha x + \beta \pmod{26}.$$

For example, let $\alpha = 9$ and $\beta = 2$, so we are working with $9x + 2$. Take a plaintext letter such as $h(= 7)$. It is encrypted to $9 \cdot 7 + 2 \equiv 65 \equiv 13 \pmod{26}$, which is the letter N. Using the same function, we obtain

$$affine \mapsto CVVWPM.$$

Classical Cryptosystems: Affine Ciphers II

- Decrypt?
- We solve the equation:

$$y = 9x + 2 \text{ and solve: } x = \tfrac{1}{9}(y - 2).$$

- We use multiplicative inverse of 9, which is 3. (9x3=1 mod 26)
- Therefore, we use the following equation:

$$x \equiv 3(y - 2) \equiv 3y - 6 \equiv 3y + 20 \pmod{26}.$$

- *V*=21, 3x21+20=83=5 (mod 26)

Classical Cryptosystems: Affine Ciphers III

- Errors:

Suppose we try to use the function $13x + 4$ as our encryption function. We obtain

$$input \mapsto ERRER.$$

If we alter the input, we obtain

$$alter \mapsto ERRER.$$

Classical Cryptosystems: Affine Ciphers Cryptanalysis

1. **Ciphertext only:** An exhaustive search through all 312 keys would take longer than the corresponding search in the case of the shift cipher; however, it would be very easy to do on a computer. When all possibilities for the key are tried, a fairly short ciphertext, say around 20 characters, will probably correspond to only one meaningful plaintext, thus allowing the determination of the key. It would also be possible to use frequency counts, though this would require much longer texts.

2. **Known plaintext:** With a little luck, knowing two letters of the plaintext and the corresponding letters of the ciphertext suffices to find the key. In any case, the number of possibilities for the key is greatly reduced and a few more letters should yield the key.

Classical Cryptosystems: Affine Ciphers Cryptanalysis II

3. **Chosen plaintext:** Choose ab as the plaintext. The first character of the ciphertext will be $\alpha \cdot 0 + \beta = \beta$, and the second will be $\alpha + \beta$. Therefore, we can find the key.

4. **Chosen ciphertext:** Choose AB as the ciphertext. This yields the decryption function of the form $x = \alpha_1 y + \beta_1$. We could solve for y and obtain the encryption key. But why bother? We have the decryption function, which is what we want.

The Vigenere Cipher

- 16th Century
- KEY: $k = (21, 4, 2, 19, 14, 17)$.
- Key and length are not known

(plaintext)	*h*	*e*	*r*	*e*	*i*	*s*	*h*	*o*	*w*	*i*	*t*	*w*	*o*	*r*	*k*	*s*
(key)	21	4	2	19	14	17	21	4	2	19	14	17	21	4	2	19
(ciphertext)	*C*	*I*	*T*	*X*	*W*	*J*	*C*	*S*	*Y*	*B*	*H*	*N*	*J*	*V*	*M*	*L*

Frequencies of letters in English

a	b	c	d	e	f	g	h	i	j
.082	.015	.028	.043	.127	.022	.020	.061	.070	.002
k	**l**	**m**	**n**	**o**	**p**	**q**	**r**	**s**	**t**
.008	.040	.024	.067	.075	.019	.001	.060	.063	.091
u	**v**	**w**	**x**	**y**	**z**				
.028	.010	.023	.001	.020	.001				

Substitution Ciphers

- Very popular
- Each letter is replaced by another letter
- Substitution cipher: Shift and affine cipher (can be broken by the frequency count)
- Permutation cipher: Vigenere and Hill ciphers

- Example
  - Encryption using substitution cipher
  - The receiver knows the permutation, so the cipher text can be decoded at the receiver

Example

- Consider the following ciphertext encoded by using permutation:

```
LWNSOZBNWVWBAYBNVBSQWVWOHWDIZWRBBNPBPOOUWRPAWXAW
PBWZWMYPOBNPBBNWJPAWWRZSLWZQJBNWIAXAWPBSALIBNXWA
BPIRYRPOIWRPQOWAIENBVBNPBPUSREBNWVWPAWOIHWOIQWAB
JPRZBNWFYAVYIBSHNPFFIRWVVBNPBBSVWXYAWBNWVWAIENBV
ESDWARUWRBVPAWIRVBIBYBWZPUSREUWRŻWAIDIREBNWIAIYV
BFSLWAVHASUBNWXSRVWRBSHBNWESDWARWZBNPBLNWRWDWAPR
JHSAUSHESDWARUWRBQWXSUWVZWVBAYXBIDWSHBNWVWWRZVIB
IVBNWAIENBSHBNWFWSFOWBSPOBWASABSPQSOIVNIBPRZBSIR
VBIBYBWRWLESDWARUWRBOPJIREIBVHSYRZPBISRSRVYXNFAI
RXIFOWVPRZSAEPRIKIREIBVFSLWAVIRVYXNHSAUPVBSVWWUU
SVBOICWOJBSWHHWXBBNWIAVPHWBJPRZNPFFIRWVV
```

Example, continued

A frequency count yields the following (there are 520 letters in the text):

W	B	R	S	I	V	A	P	N	O	...
76	64	39	36	36	35	34	32	30	16	...

e	t	a	o	i	n	s	h	r
.127	.091	.082	.075	.070	.067	.063	.061	.060

Table 2.2: Frequencies of Most Common Letters in English

Example, continued

	W	B	R	S	I	V	A	P	N
W	3	4	12	2	4	10	14	3	1
B	4	4	0	11	5	5	2	4	20
R	5	5	0	1	1	5	0	3	0
S	1	0	5	0	1	3	5	2	0
I	1	8	10	1	0	2	3	0	0
V	8	10	0	0	2	2	0	3	1
A	7	3	4	2	5	4	0	1	0
P	0	8	6	0	1	1	4	0	0
N	14	3	0	1	1	1	0	7	0

Table 2.3: Counting Digrams

Example, continued

The letter n has the property that around 80% of the letters that precede it are vowels. Since we already have identified W, S, I, P as vowels, we see that R and A are the most likely candidates. We'll have to wait to see which is correct.

The letter h often appears before e and rarely after it. This tells us that $N = h$.

L W N S O Z B N W V W B A Y B N V B S
e h o t h e s e l r t h s t o

Q W V W O H W D I Z W R B B N P B P ...
e s e e i e n t t h a t a ...

we hold these truths to be self evident that all men are created equal that they are endowed by their creator with certain unalienable riglits that among these are life liberty and the pursuit of happiness that to secure these rights governments are instituted among men deriving their just powers from the consent of the governed that whenever any form of government becomes destructive of these ends it is the right of the people to alter or to abolish it and to institute new government laying its foundation on such principles and organizing its powers in such form as to seem most likely to effect their safety and happiness

Sherlock Holmes, “The adventures of dancing men”

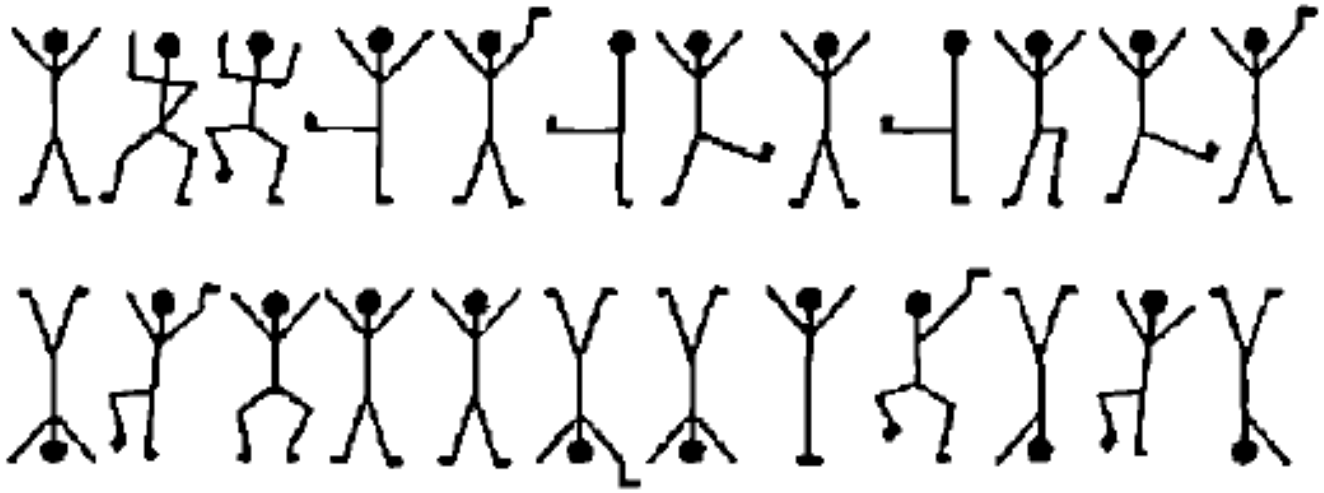
- Letter from Mr. Cubitt (married to Ms Patrick) to Mr. Holmes. Message is found in his garden at his Manor

- Two weeks later, Mr Cubitt finds another series of figures written in chalk on his toolhouse door:

- Three days later, another message:

- Mr Cubitt gives copies of all of these to Holmes.
- Holmes sends a telegram to someone. No reply for two days.
- Another message received by Cubitt

- Another message received by Mr. Cubitts



- Holmes arrives at Mr. Cubitts house next day, he and his wife is shot dead.
- Holmes got reply to his telegram and says the matter is very urgent

Decryption of the message

- Most common figure is: likely to be E
-
- Fourth message decoded as _ E_ E
  - Holmes guessed it to be NEVER out of (LEVER, NEVER, SEVER)