

Names: Yasar Azimi

Assignment 1

Dr.Abdalrahman Alfagi

Class: ITC 370

2023/10/6

1. **What is Cryptography**?

Answer: Cryptography is the study of encrypting and decrypting information, so that aside from the receiver and sender no one else gets access to the information or understand it if they somehow do get access to it.

1. **Basic terminology in cryptography:**

Answer: Some of the basic terminology that we have read so far includes:

1. **Cipher**: the algorithm we use to change plain text to a cipher text.
2. **Cipher text**: the encrypted message.
3. **Decipher**: change the cipher text back to the normal/original message using the key.
4. **Plain Text**: the original message.
5. **Enciphe**r: Change a normal message to cipher text using the algorithm and the key.
6. **Key**: the information used to encrypt and decrypt the (messages/text/files/emails).
7. **Security services:**

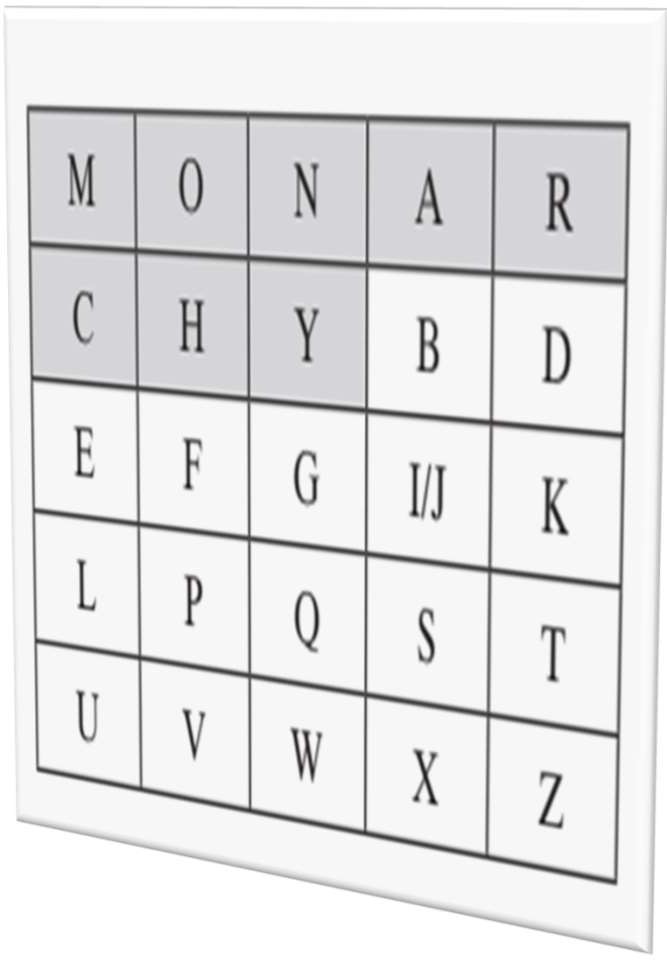
Answer: Security services are services that are provided to ensure the protection of a certain communication, connection and the messages authenticity. We have six sub topics included in security services here.

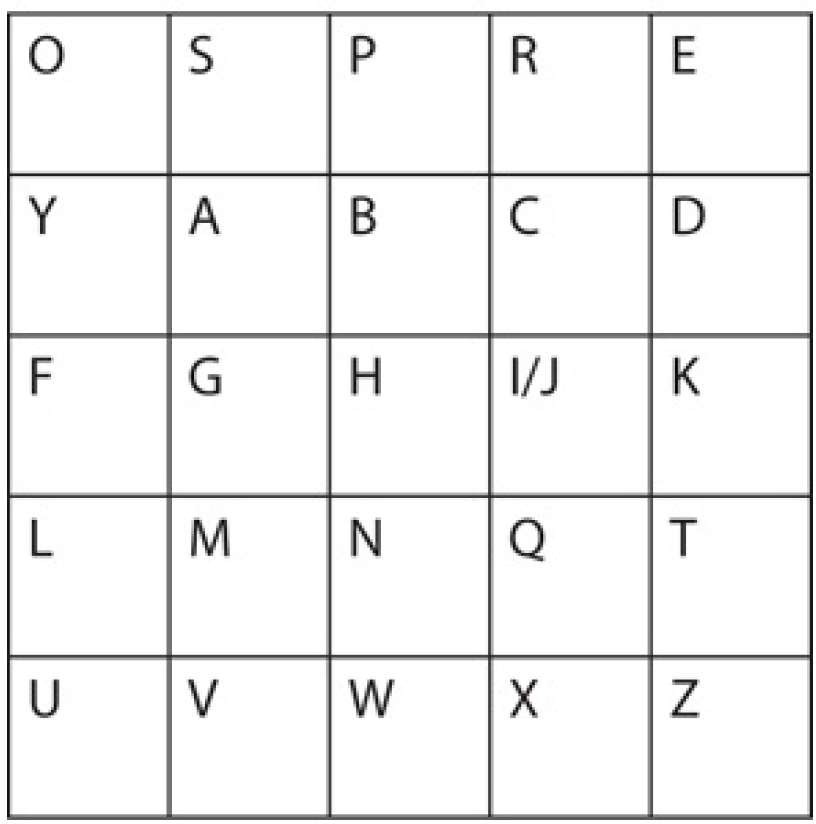
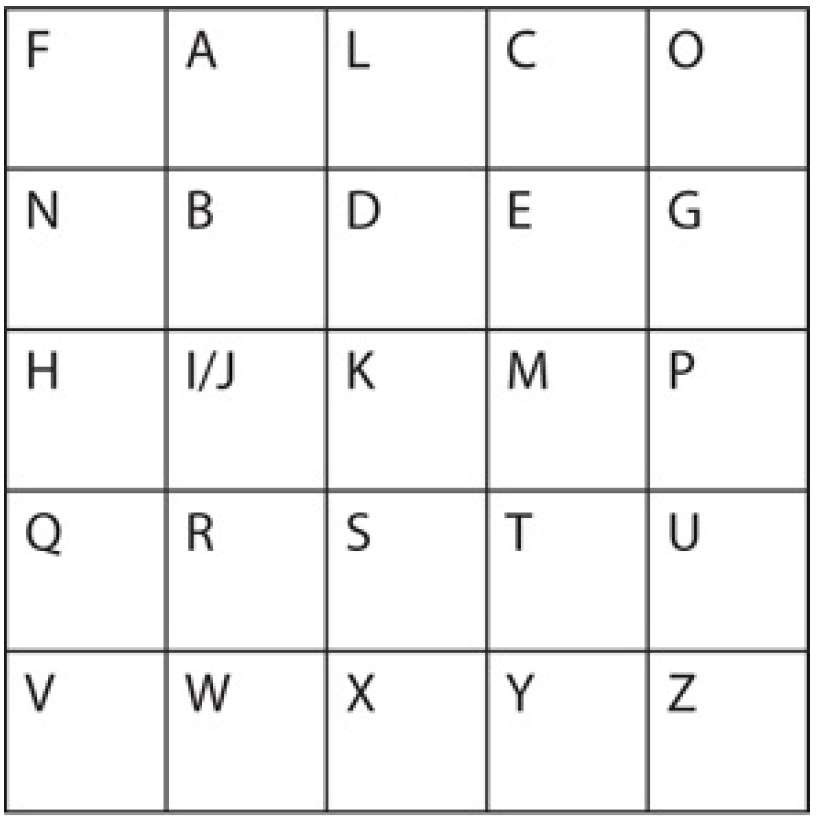
1. **Authentication**: Whether the message is real or not (its content is what they say it is), or the message has been sent from another address
2. **Confidentiality**: How secure the connection is.
3. **Integrity**: If the data is as told by the sender and not something else.
4. **Non**-**repudiation**: The assurance that your data is secure.
5. **Availability**: How your connection is available to others.
6. **Access** **Control**: How easy is it to gain access to your data or connection.
7. **Categories of Cryptography**:

Answer: We have two types of cryptography which includes Symmetric and Asymmetric and Hashing.

1. **Symmetric**: The type of cryptography in which the key used for encrypting and decrypting the data is the same.
2. **Asymmetric**: The type of cryptography in which the key used for encrypting is different than the one used for decrypting.
3. **Classical Cryptography**:

Answer: We have two types of classical cryptography Substitutions cypher and transposition cypher.

1. **Substitutions cypher**: In substitution cypher the letters are replaced by other letters.
2. **Transposition cypher**: In transposition cypher the letters are arranged in different order.
3. **Caeser cypher:** Created by Julius Caesar and first used in military affairs, the way to use it is by replacing each letter by the 3rd letter, it has 25 possible keys.
4. **Mono alphabetic:** It’s known as the simple substitution cypher, which relies on a fixed replacement structure. So if “A” is changed to “R” the in plaintext A is always change to “r”. The amount of possible keys is”4 x 10^26 possible keys”.
5. **Atbash cypher:** It is a simple substitution cipher that was made originally for the Hebrew alphabet. It’s a simple cipher that works by reversing the order of the alphabet.
6. **Playfair cypher:** It is invented in 1854 by Charles wheatstone, and was used in World War 1 and World War 2. It’s based on the use of 5\*5 matrix using keywords. 
7. **Two-square cypher:** This cypher is known as the double playfair, and works on diagraphs. Unlike playfair which needs one square this one needs two squares with each needing their own keywords.



1. **Four square cypher**: It uses the same concept as the two square cipher and is encrypted using the 5x5 letter square. They upper left and lower right matrices are the plaintext square.

