NETWORK SECURITY CRYPTOGRAPHY

By Ravi Teja

- *WHAT IS NETWORK*
  A network is an interconnection or a media between two or more systems to share information among them.
  ∗ The various threats caused to network are : Remote Login, Application Backdoors, SMTP Session Hijackings, Operating System Bugs, Spams ,Viruses etc.

SECURITY USED TO BE AN INCONVENIENCE SOMETIMES, BUT NOW IT'S A NECESSITY ALL THE TIME.

NETWORK SECURITY ?

The security provided to the network is called network security which at present is looming on horizon as a massive problem.

There are two kinds of Network Security mainly as :

☐ Transit Security :

It just encrypts the packets to be transferred.

☐ Traffic Security :

It acts just as a screen between hosts & remote sites.

How does network security works?

Network security across an organization fall into two general categories:

Access control

Threat control

What are the key tools of network security?

A multi-layered approach to network security implements controls at numerous points within a network to provide comprehensive access control and threat control.

Firewall : A firewall establishes a barrier between the trusted and the untrusted areas of a network.

Load Balancer : A load balancer distributes load based on metrics.

IDS/IPS : The classic IDS/IPS is deployed behind a firewall and provides protocol analysis and signature matching on various parts of a data packet.

Sandbox : A sandbox is similar to an IDS/IPS, except that it does not rely on signatures. A sandbox can emulate an end-system environment and determine if a malware object is trying, for example, to execute port scans.

NTA/NDR : NTA/NDR looks directly at traffic (or traffic records such as NetFlow) and uses machine learning algorithms and statistical techniques to evaluate anomalies and determine if a threat is present.

PROBLEMS & ATTACKS

There are few intertwined areas in network security as:

□ Secrecy

□ Authentication

□ Non-Repudiation

□ Integrity Control etc.

∗ The threats are classified into two categories :

Passive Attacks :

A passive attack is one in which the attacker eavesdrops and listens to the message but can’t modify the message.

Active Attacks :

An active attack is one in which the attacker modifies, deletes, replay or introduce new messages into the stream of message.

CRYPTOGRAPHY

* Cryptography is the ability to send information between particulars in a way that it prevents others from reading the data.

* The data is transferred by applying two techniques by changing the plain text & Cipher texts as Encryption (P to C) & Decryption (C to P).

PRINCIPLES & SERVICES OF CRYPTOGRAPHY

The two fundamental principles of cryptography are:

□ Messages must contain some Redundancy (information not needed to understand the message).

□ Some method is needed to foil replay attacks (validation of messages by timestamp) i.e. freshness.

∗ The services provided by the cryptography are as follows:

□ Integrity Checking

□ Authentication

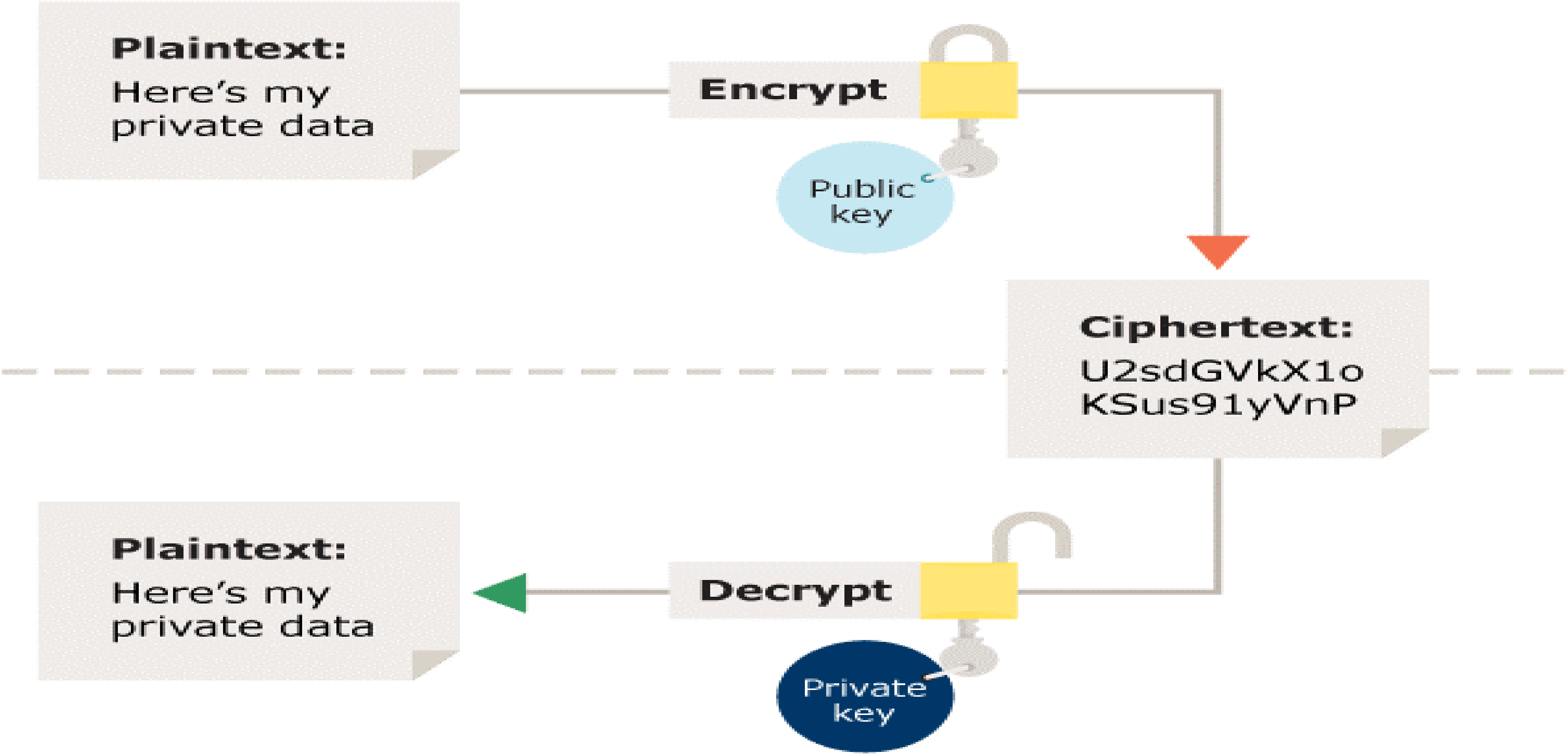
□ Protection to the data

□ Confidentiality of information etc.

ENCRYPTION & DECRYPTION

* The way of converting the plain text to the cipher text by the means of few keys is called as “encryption”.

* The way of converting the cipher text to the plain text by the use of keys that are suitable to it is called as “decryption”.



Plaintext:
Here's my private data

Encrypt

Public key

Ciphertext:
U2sdGVkX1o
KSus91yVnP

Decrypt

Private key

Plaintext:
Here's my private data

Reference:

* https://www.wikipedia.org/

* https://www.slideshare.net

Thank you..