National Institute of Technology, Warangal

(*Department of Computer Science Engineering*)

Introduction to Security

Lecture By:-
Dr R Padmavathy
Dept of CSE, NIT Warangal

1. Secure Aggregation Protocol using Homomorphic Encryption to solve privacy problems in federated learning
2. Secure Exchange of ML models using Blockchain technology

Content

1. What is Security?
2. Kerckhoffs' Principles
3. OSI Security Architecture
4. Threats and Attacks
5. Cryptographic Security
8. Security Services
9. Security Mechanism
10. Flow of Secure System
11. Layers in Secure System
12. Protocol Stack.

Cryptographic Algorithm

Any encrpytion scheme(Gen, Enc, Dec) is defined by three algorithms:

Gen (*key generation algorithm*) : is a probabilistic algorithm that outputs a key k chosen according to some distribution.

Enc (*encryption algorithm) :* takes as input a key k and a message and outputs a ciphertext c.

$$C \leftarrow Enc_k(m)$$

Dec (decryption algorithm) : takes as input a key and a ciphertext and outputs a message m.

$$m := Dec_k(c)$$

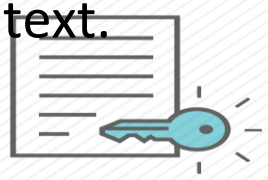
What is Security ?

Definition 1: An encryption scheme is secure if no adversary can find the secret key when given a cipher text.

Definition 2: An encryption scheme is secure if no adversary can find the plaintext that corresponds to the cipher text.

Definition 3: An encryption scheme i s secure if no adversary can determine any character of the plaintext that corresponds to the cipher text.

Definition 4: An encryption scheme is secure if no adversary can derive any meaningful information about the plaintext from the cipher text.



What is Security ?

Definition 5: An encryption scheme is secure if no adversary can compute any function of the plaintext from the cipher text.

Kerckhoffs' Principles

Principle 1: The cipher method must not be required to be secret.

Principle 2: The adversary knows the algorithm.

Principle 3: The only secret is the key.

OSI Security Architecture

The OSI security architecture focuses on *security attacks*, *mechanisms*, and *services*. These can be defined briefly as follows:

- **Security attack:** Any action that compromises the security of information owned by an organization.

- **Security mechanism:** A process (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security attack.

- **Security service:** A processing or communication service that enhances the security of the data processing systems and the information transfers of an organization.

Threats and Attacks

Threats:

A threat is a possible danger that might exploit a vulnerability.

Attacks:

An assault on system security that derives from an intelligent threat.

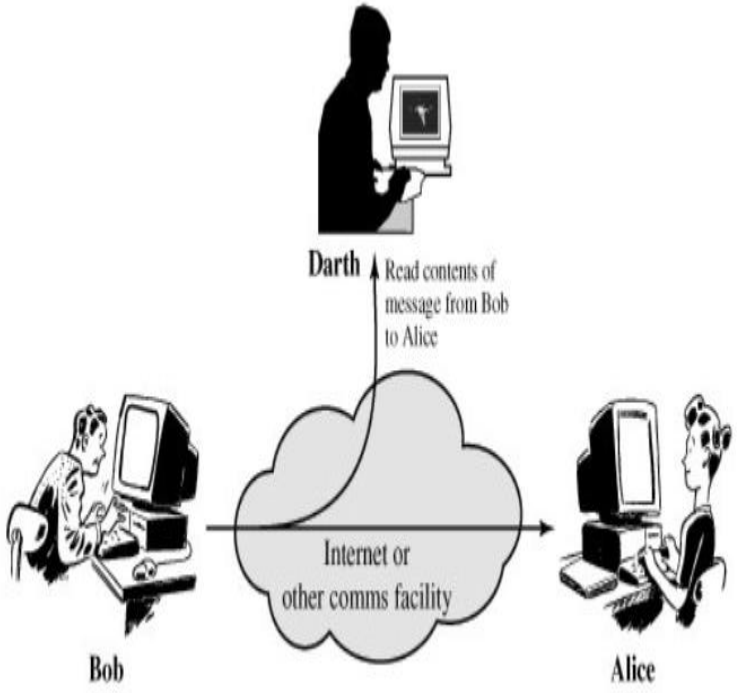
Types of Attacks:

1. Passive Attacks,
2. Active Attacks.

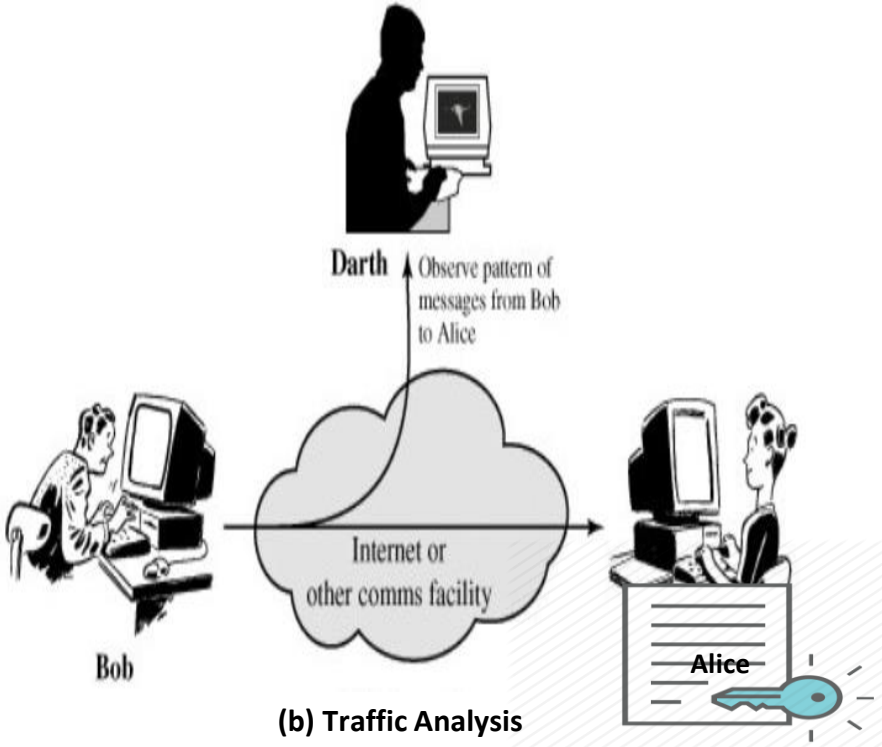
Security Attacks

Passive Attacks:

A passive attack attempts to learn or make use of information from the system but does not affect system resources.



(a) Release of message contents

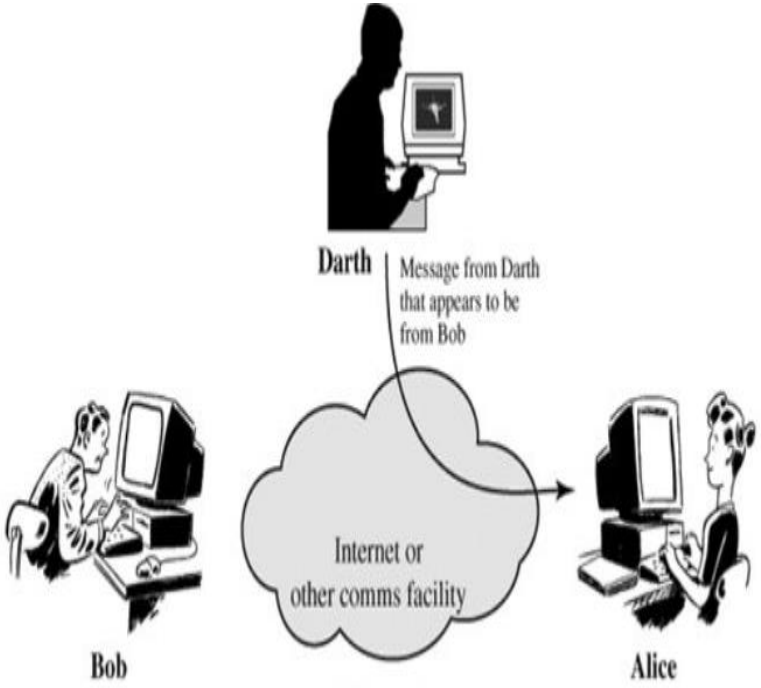


(b) Traffic Analysis

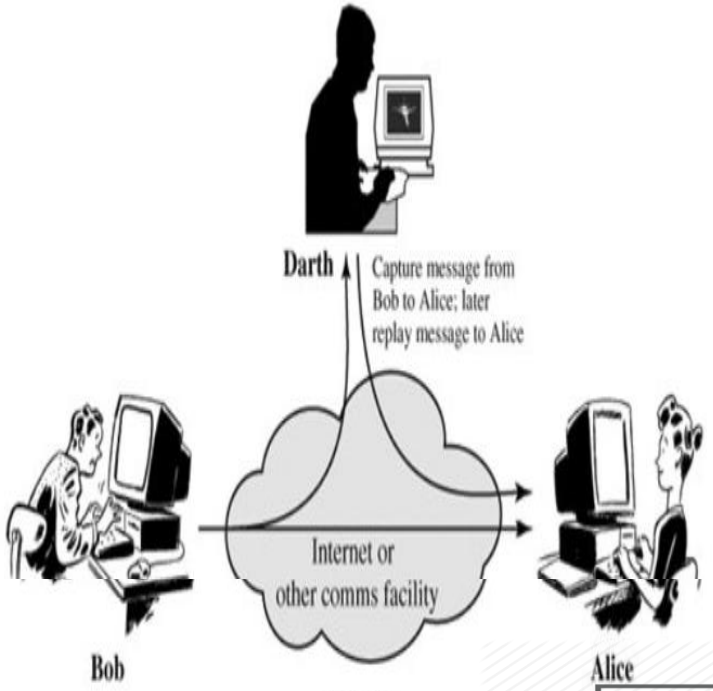
Security Attacks

Active Attacks:

An active attack attempts to alter system resources or affect their operation.



(a) Masquerade

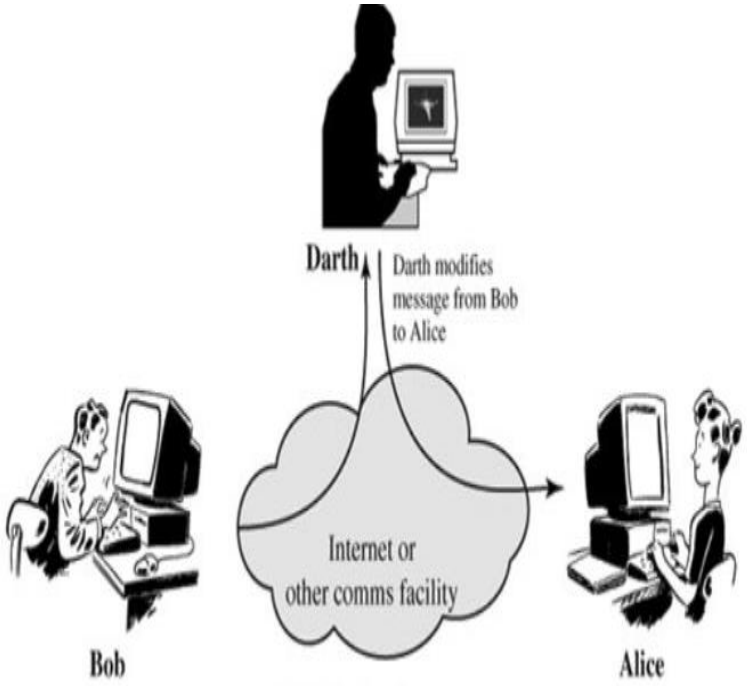


(b) Reply

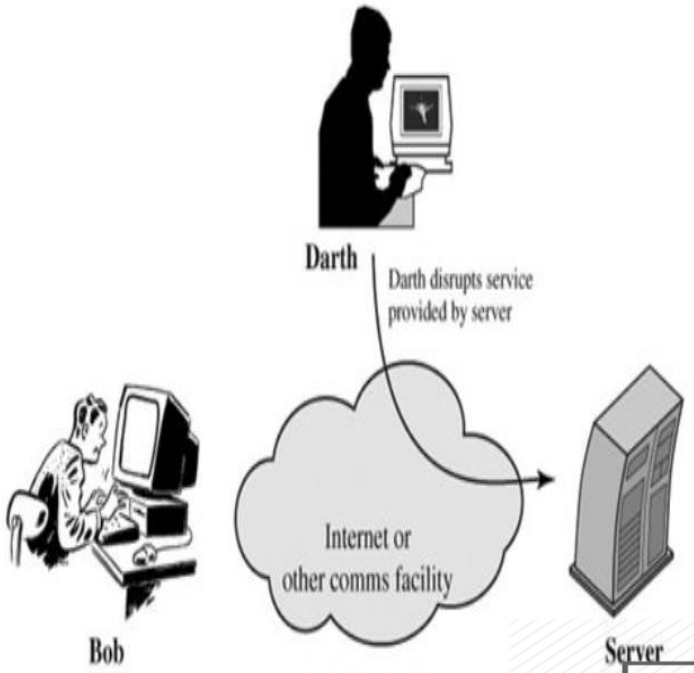
Security Attacks

Active Attacks:

An active attack attempts to alter system resources or affect their operation.



(c) Modification of Message



(d) Denial of Service

Cryptographic Security

How can we develop strong cryptosystems **that can be practically used?**

- Should be based on **strong** mathematical primitives.
- Should be able to resist **known attacks.**

Cryptographic Security (Attacks)

1. **Mathematical attacks**

   Exploiting flaws in mathematical construction, solving system as set of mathematical equations, extracting information regarding key.

2. **Statistical attacks**

   Extracting information from cipher text, exploiting randomness properties for distinguishing attacks.

Cryptographic Security (Attacks)

China's Sunway Taihulight Supercomputer

124.5 petaflops peak performance (10.65 million compute cores)

Cryptographic Security (Attacks)

3. Computational attacks

Using high-performance systems for attacks, solving system using a different model of computation.

4. **Implementation & side-channel attacks**

Extracting information about key from physical processes (power, magnetic field, time consumption), from equipment or memory, using fault injection, hardware tampering.

Cryptographic Security (Attacks)

- The block cipher **DES** with **56-bit keys**, allows attacks via **exhaustive search** and is not currently secure.

- The Wired Equivalent Privacy (**WEP**) algorithm (40&128 bit) is used to protect wireless communication & prevent unauthorized access to a wireless network.
  WEP uses RC4 stream cipher & is subject to attacks due to **flaws in its design**

Cryptographic Security (Attacks)

Example – Skipjack

- **Block cipher** developed by the US NSA.
- Uses a **80-bit key** to encrypt and decrypt **64-bit data blocks**.
- Based on **unbalanced Feistel network** with **32 rounds.**

Cryptographic Security (Attacks)

Attacks on Skipjack

- **Impossible differential cryptanalysis** (31 rounds) : slightly faster than exhaustive search.
- **Saturation attack** (27 rounds): User key can be recovered with **250 chosen plaintexts** & **3.275 encryption times**.
- Truncated differential attack, related-key miss-in-themiddle attack, related-key rectangle attack.
- **FSE-2016:** Statistical integral distinguisher – key recovery attack on **Skipjack variant**.

Not recommended for current use (NIST, ECRYPT II).

Security Services

Definition:

A processing or communication service that is provided by a system to give a specific kind of protection to system resources.

- Security Services implement security policies and are implemented by security mechanisms.

These services are divided into five categories:

1. Authentication,
2. Access Control,
3. Data Confidentiality,
4. Data Integrity,
5. Non Repudation.

Security Services

1. Authentication:

The authentication service is concerned with assuring that a communication is authentic.

2. Access Control:

Access control is the ability to limit and control the access to host systems and applications via communications links. To achieve this, each entity trying to gain access must first be identified, or authenticated, so that access rights can be tailored to the individual.

3. Data Confidentiality:

The protection of data from unauthorized disclosure.

Security Services

4. Data Integrity:

The assurance that data received are exactly as sent by an authorized entity (i.e., contain no modification, insertion, deletion, or replay).

5. Non-Repudiation:

Provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication.

Security services in detail

Authentication

1. Peer Entity Authentication:
2. Data Origin Authentication

Access Control

Data Confidentiality
1.Connection Confidentiality
2.Connectionless Confidentiality
3.Selective field Confidentiality
4.Traffic flow Confidentiality

Security services in detail

Data Integrity

1. Connection Integrity with recovery
2. Connection Integrity without recovery
3. Selective field connection Integrity
4. Connectionless Integrity
5. Selective field connectionless integrity

Non repudiation

1.Origin
2.Destination

Availability

Security Mechanism

1. Encipherment
2. Digital Signature
3. Access Control mechanisms
4. Data Integrity MAC HMAC
5. Authentication Exchange X and Z X wants to authenticate Z
6. Traffic Padding
7. Routing Control
8. Notarization

SERVICE	Encryption	Digital Signature	Access control	Data Integrity	Authentication exchange	Traffic padding	Routing control	notarization
Peer entity authentication	Y	Y			Y			
Data origin authentication	Y	Y						
Access Control			Y					
Confidentiality	Y						Y	
Traffic flow confidentiality	Y					Y	Y	
Data Integrity	Y			Y				
Non repudiation		Y						Y

Network security model

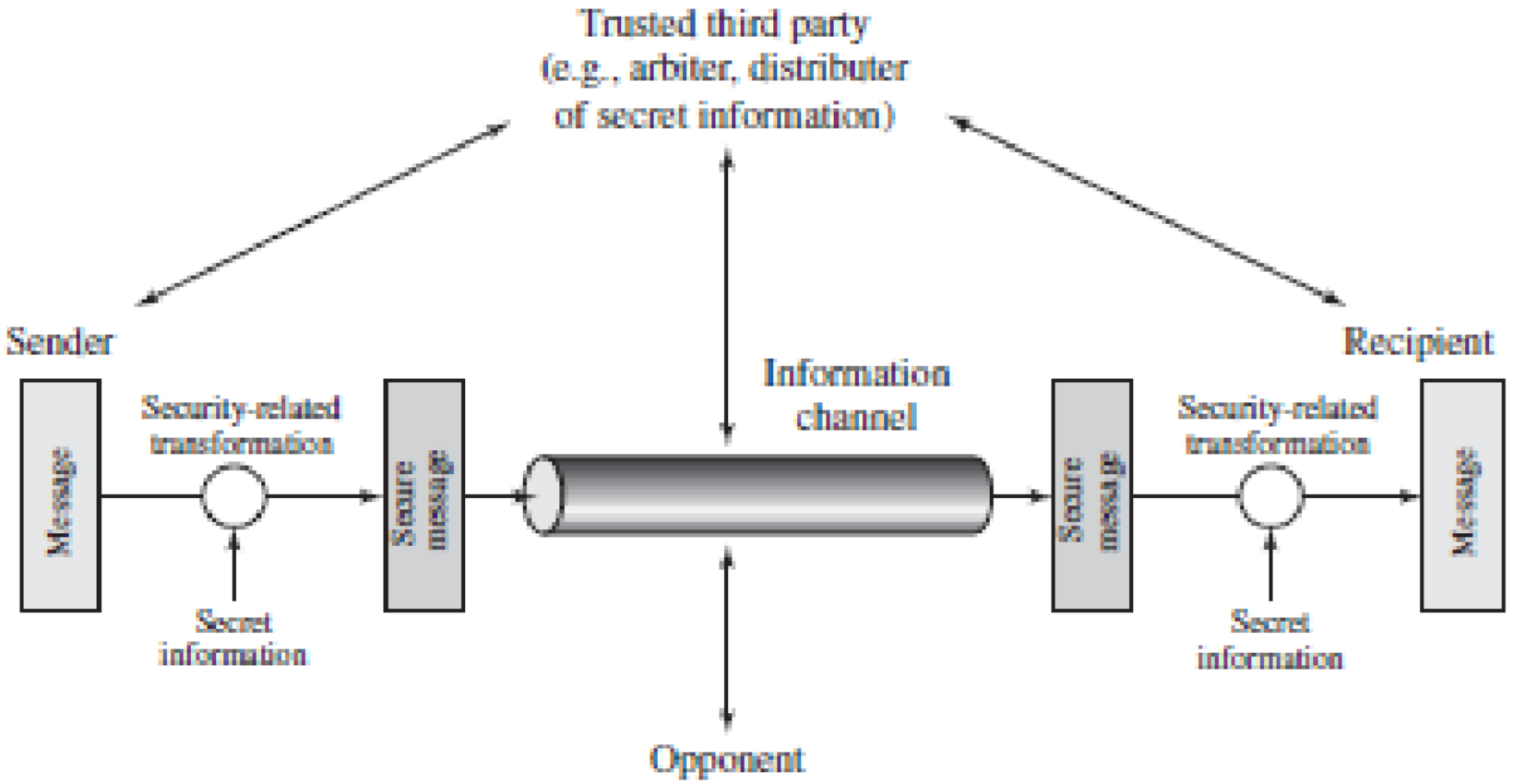


Figure 1.4 Model for Network Security

Steps in Network Security Model

1. **Design an algorithm for security related transformation – Adversary should not succeed his goal**

1. **Generate secret information**

1. **Distribution and sharing of secret information**

1. **Specify a protocol to be used by two principles make use of security algorithm and secret information to achieve specific security services**

Network Access Control model

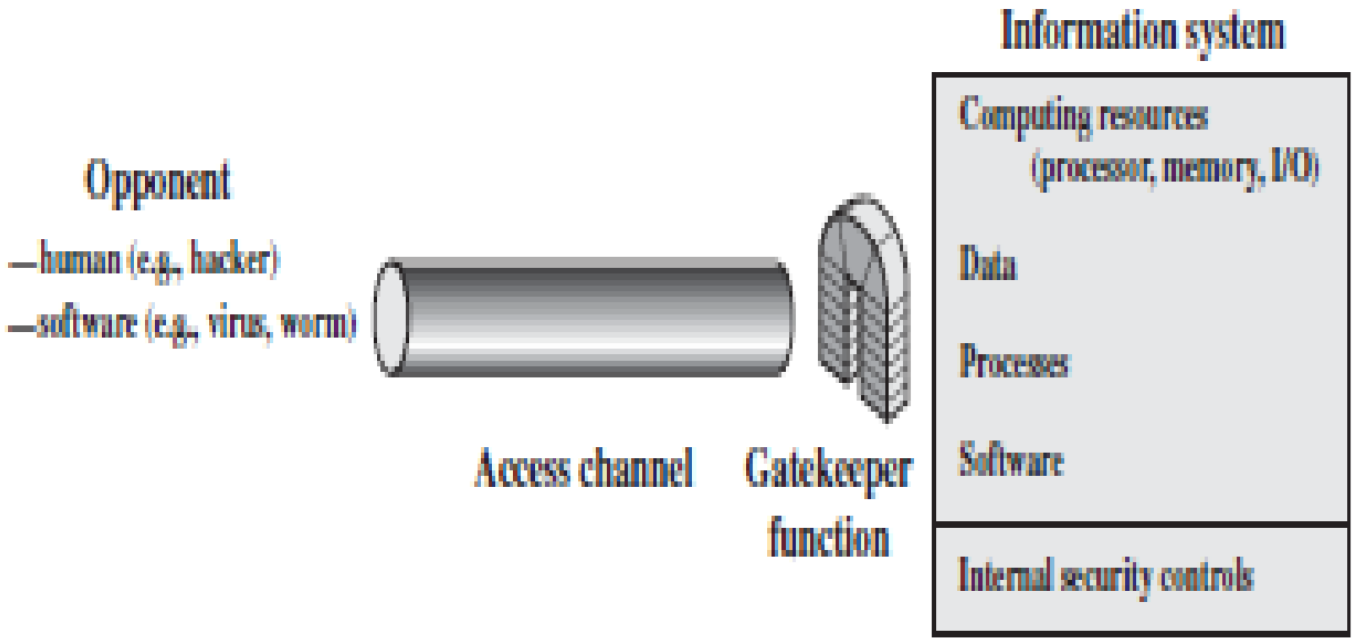
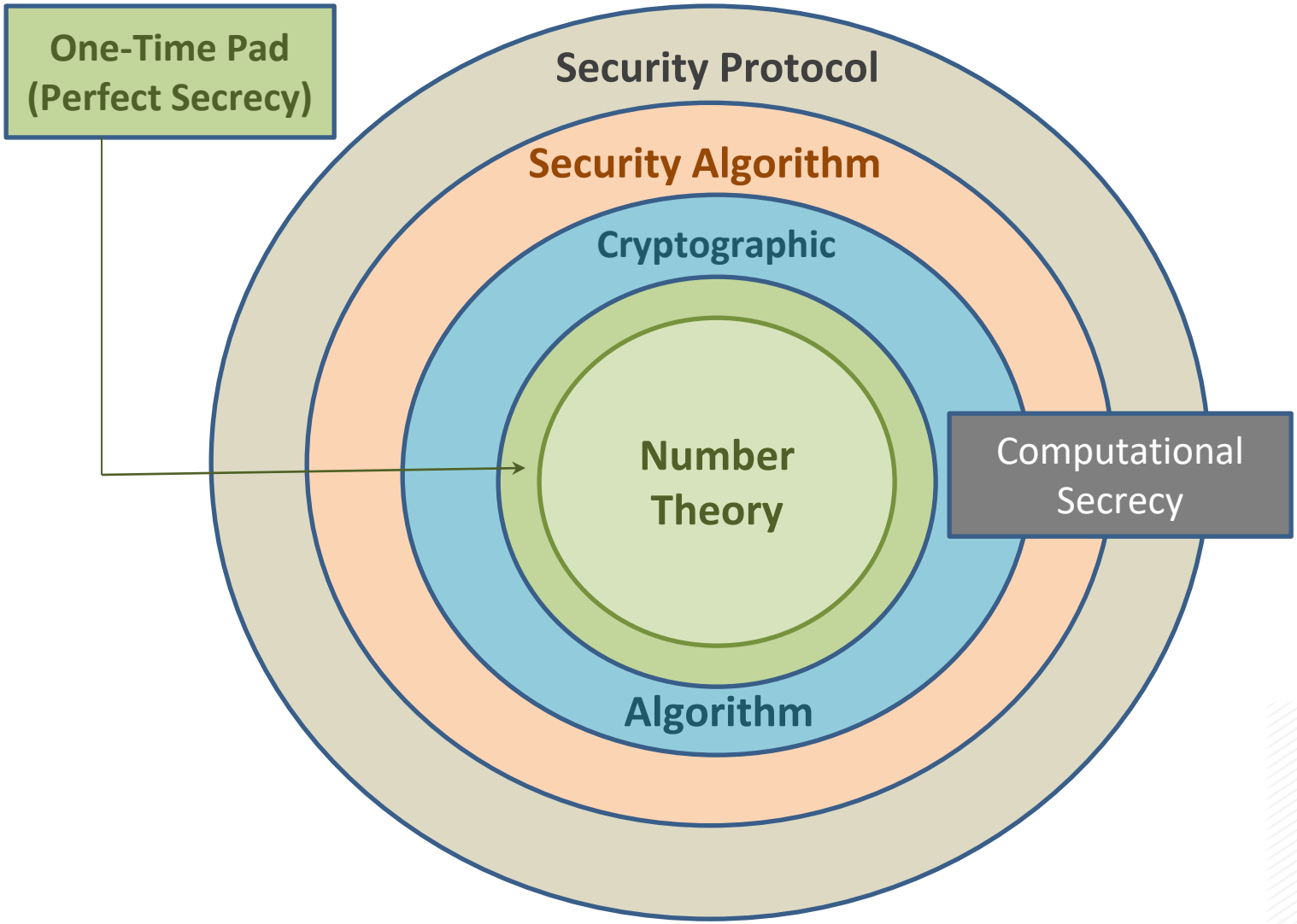


Figure 1.5 Network Access Security Model

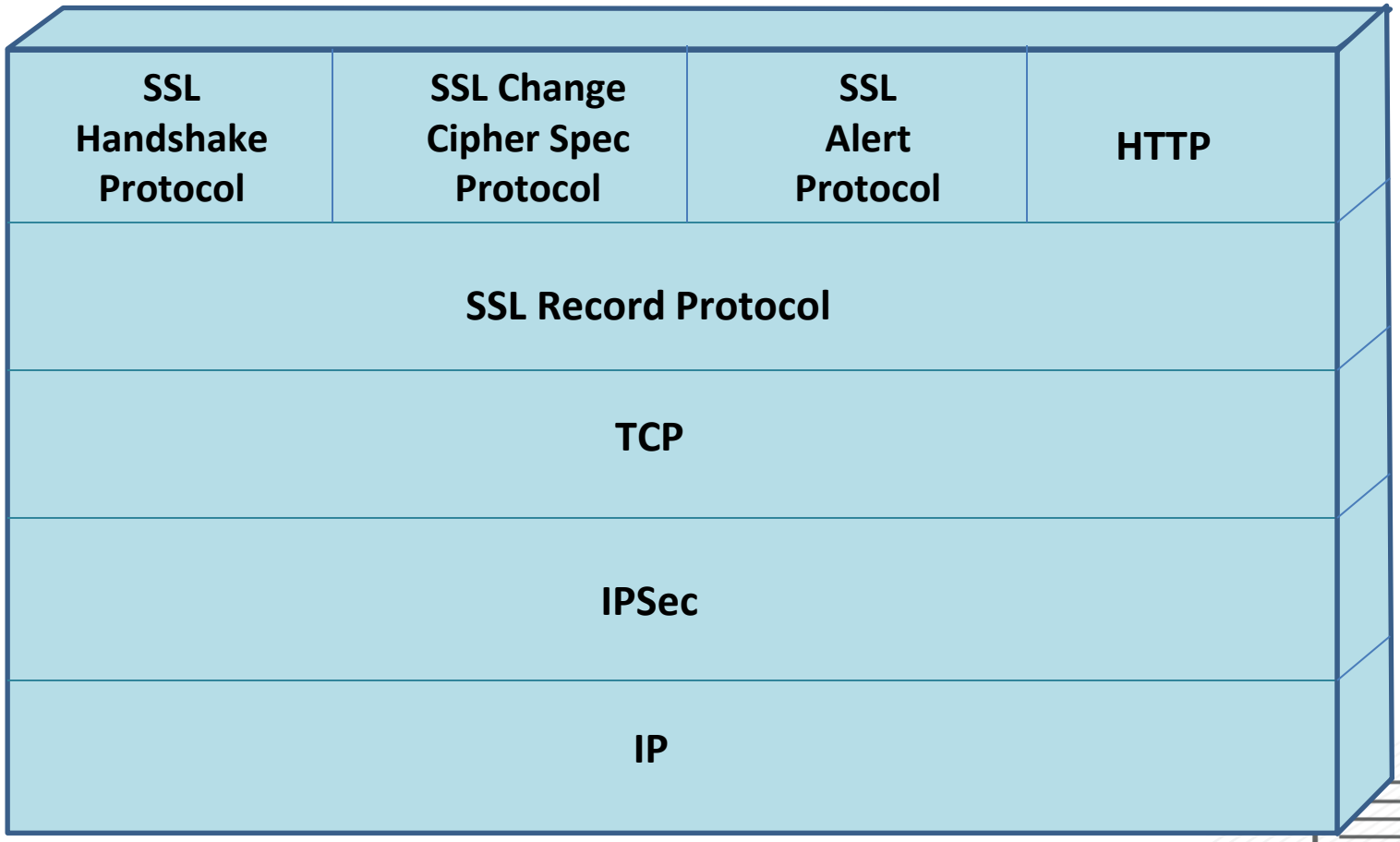
Flow of Secure System

Mathematical Foundation	Cryptographic Algorithm	Security Algorithm	Security Protocol
1.Number Theory	1.Stream Cipher (e.g. RC4, AS5/1)	1.RSA-Digital Signature	1.PGP
2. Abstract Algebra	2. Block Cipher (e.g. DES, AES)	2. ElGamal- Digital Signature	2. Kerberos
3.Computational Number Theory	3.Public key Cryptography (e.g. RSA, ElGammal)	3.DSS / DSA	3.SSL / TSL
		4. Certificate	4.IPSec
			5.Wireless Security Protocol (WEP)

Layers in Secure System



Protocol Stack



Any Queries ?

Thank You…