Cryptography

Cryptography

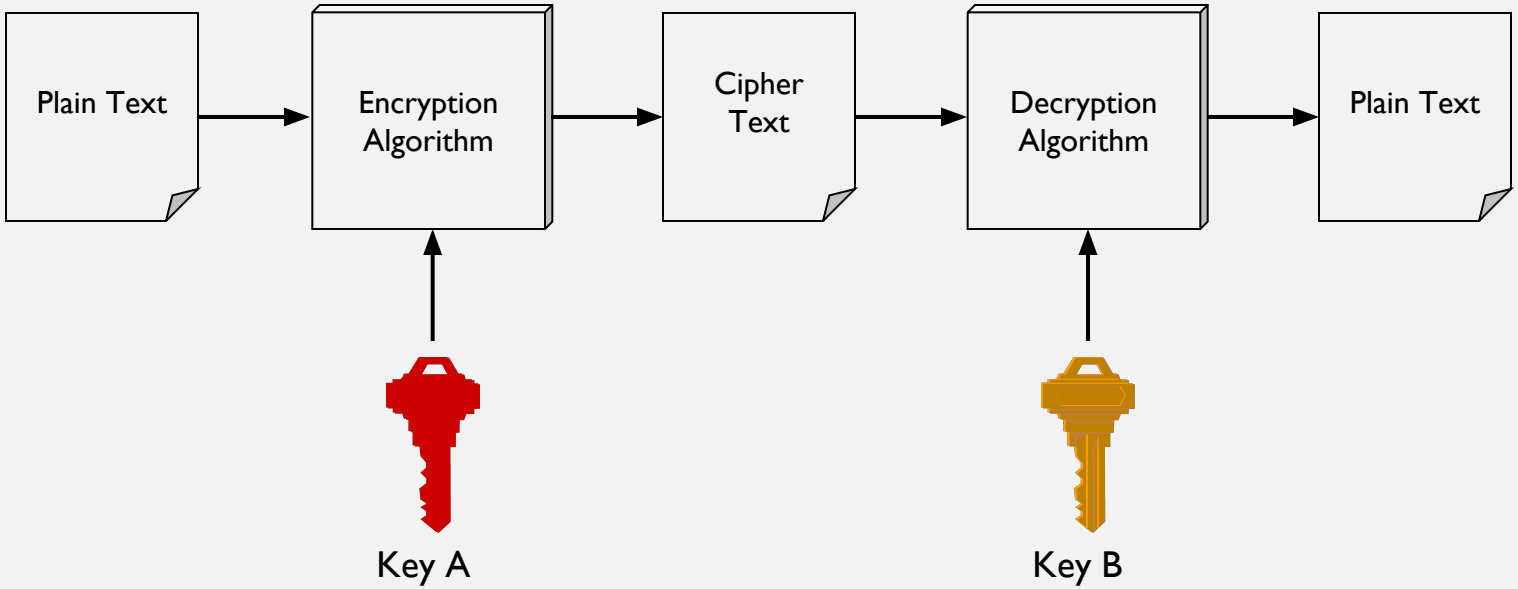
Basics

- Cryptography is the science of secret, or hidden writing
- It has two main Components:
  1. Encryption
     - Practice of hiding messages so that they can not be read by anyone other than the intended recipient.
  2. Authentication & Integrity
     - Ensuring that users of data/resources are the persons they claim to be and that a message has not been altered.

Encryption

Cipher

- Cipher is a method for encrypting messages



- Encryption algorithms are standardized & published
- The key which is an input to the algorithm is secret
  - Key is a string of numbers or characters
  - If same key is used for encryption & decryption the algorithm is called symmetric
  - If different keys are used for encryption & decryption the algorithm is called asymmetric

Encryption

Symmetric Algorithms

- Algorithms in which the key for encryption and decryption are the same are Symmetric
  - Example: Caesar Cipher
- Types:
  1. Block Ciphers
     - Encrypt data one block at a time (typically 64 bits, or 128 bits)
     - Used for a single message
  2. Stream Ciphers
     - Encrypt data one bit or one byte at a time
     - Used if data is a constant stream of information

Symmetric Encryption

Key Strength

- Strength of algorithm is determined by the size of the key
  - The longer the key the more difficult it is to crack
- Key length is expressed in bits
  - Typical key sizes vary between 48 bits and 448 bits
- Set of possible keys for a cipher is called key space
  - For 40-bit key there are 2^{40} possible keys
  - For 128-bit key there are 2^{128} possible keys
  - Each additional bit added to the key length doubles the security
- To crack the key the hacker has to use brute-force

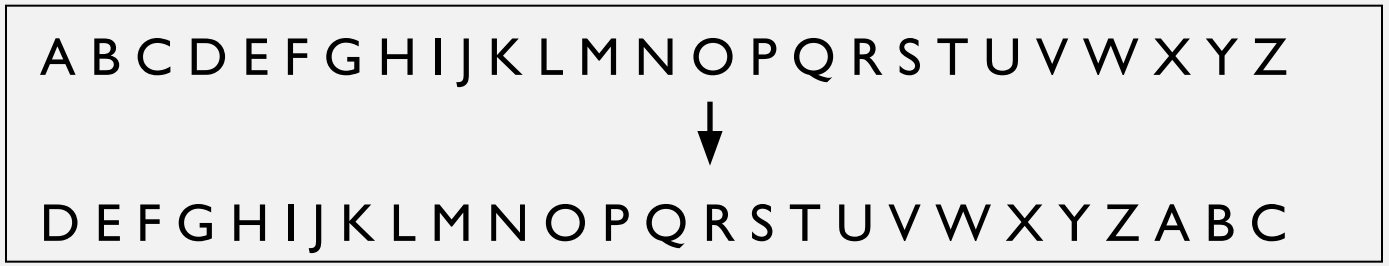
  (i.e. try all the possible keys till a key that works is found)
  - Super Computer can crack a 56-bit key in 24 hours
  - It will take 2^{72} times longer to crack a 128-bit key

  (Longer than the age of the universe)

Substitution Ciphers

Caesar Cipher

- Caesar Cipher is a method in which each letter in the alphabet is rotated by three letters as shown



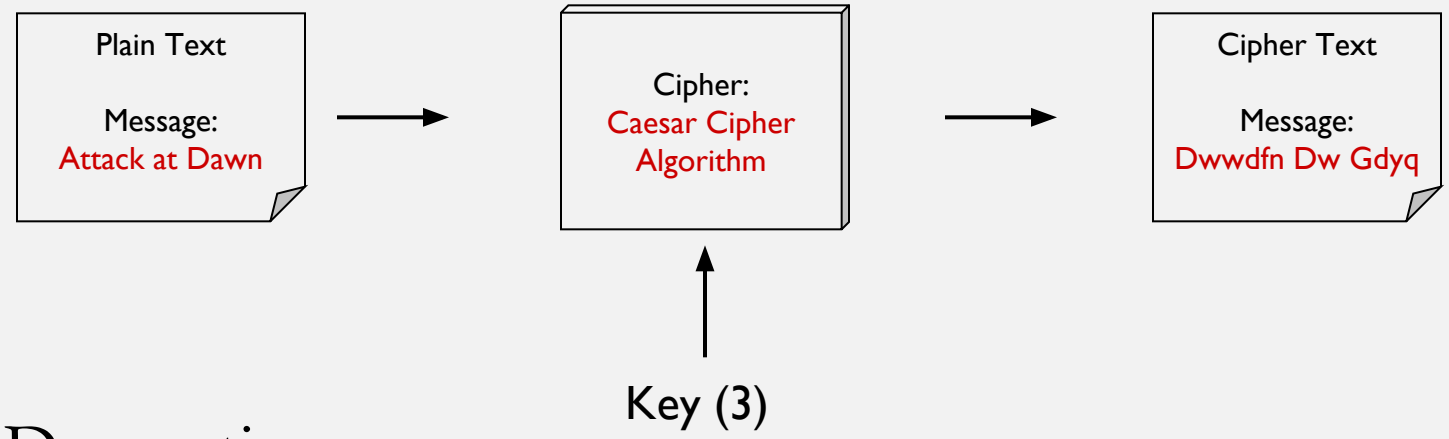
- Let us try to encrypt the message
  - Attack at Dawn

Assignment: Each student will exchange a secret message with his/her closest neighbor about some other person in the class and the neighbor will decipher it.

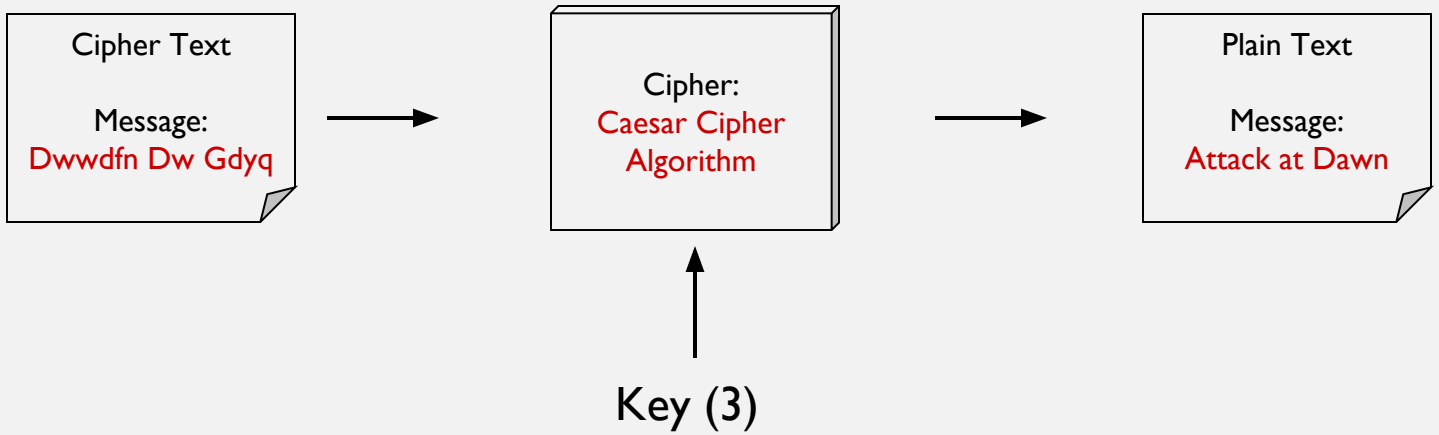
Substitution Ciphers

Caesar Cipher

Encryption



Decryption



How many different keys are possible?

Substitution Cipher

Monoalphabetic Cipher

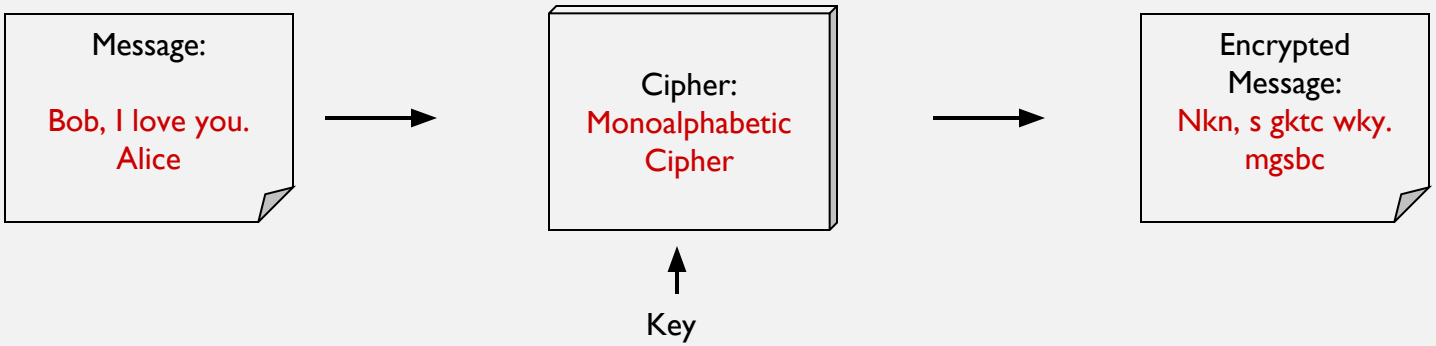
- Any letter can be substituted for any other letter
  - Each letter has to have a unique substitute

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

↓

M N B V C X Z A S D F G H J K L P O I U Y T R E W Q

- There are 26! pairing of letters ($\sim 10^{26}$)
- Brute Force approach would be too time consuming
  - Statistical Analysis would make it feasible to crack the key



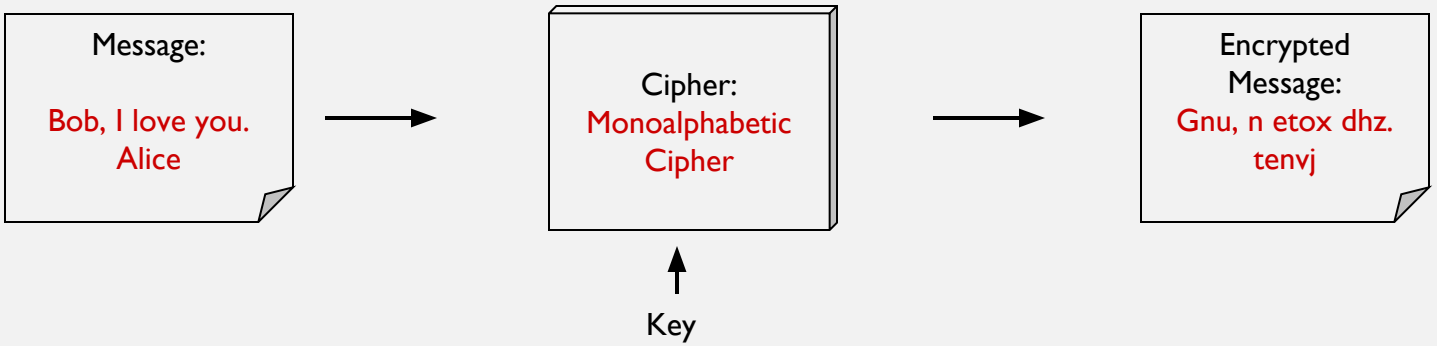
Substitution Cipher

Polyalphabetic Caesar Cipher

- Developed by Blaise de Vigenere
  - Also called Vigenere cipher
- Uses a sequence of monoalpabetic ciphers in tandem
  - e.g. C_1, C_2, C_2, C_1, C_2

Plain Text	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
	↓
C1(k=6)	F G H I J K L M N O P Q R S T U V W X Y Z A B C D E
C2(k=20)	T U V W X Y Z A B C D E F G H I J K L M N O P Q R S

- Example

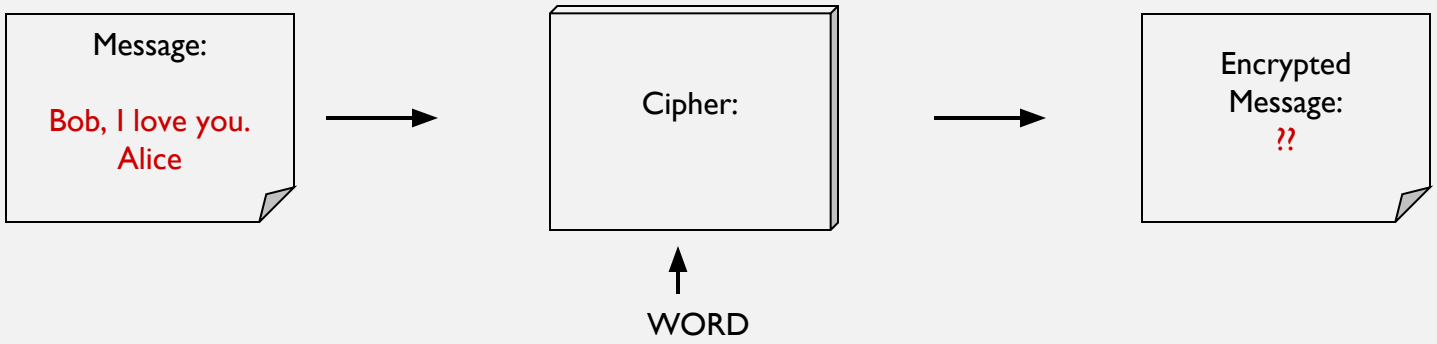


Substitution Cipher

Using a key to shift alphabet

- Obtain a key to for the algorithm and then shift the alphabets
  - For instance if the key is word we will shift all the letters by four and remove the letters w, o, r, & d from the encryption
- We have to ensure that the mapping is one-to-one
  - no single letter in plain text can map to two different letters in cipher text
  - no single letter in cipher text can map to two different letters in plain text

Plain Text	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
	↓
C1(k=6)	W O R D A B C E F G H I J K L M N P Q S T U V X Y Z



Vigenere Cipher

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Cryptanalysis

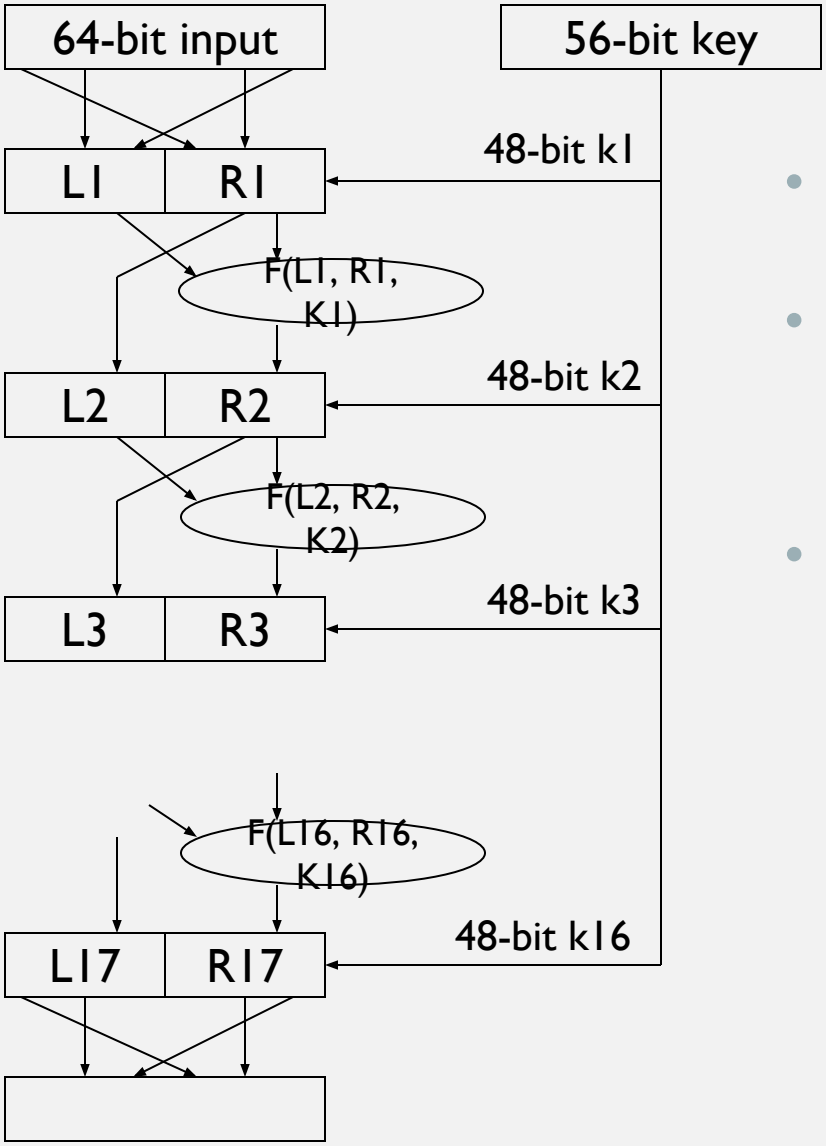
Techniques

- Cryptanalysis is the process of breaking an encryption code
  - Tedious and difficult process
- Several techniques can be used to deduce the algorithm
  - Attempt to recognize patterns in encrypted messages, to be able to break subsequent ones by applying a straightforward decryption algorithm
  - Attempt to infer some meaning without even breaking the encryption, such as noticing an unusual frequency of communication or determining something by whether the communication was short or long
  - Attempt to deduce the key, in order to break subsequent messages easily
  - Attempt to find weaknesses in the implementation or environment of use of encryption
  - Attempt to find general weaknesses in an encryption algorithm, without necessarily having intercepted any messages

Data Encryption Standard (DES) Basics

- Goal of DES is to completely scramble the data and key so that every bit of cipher text depends on every bit of data and ever bit of key
- DES is a block Cipher Algorithm
  - Encodes plaintext in 64 bit chunks
  - One parity bit for each of the 8 bytes thus it reduces to 56 bits
- It is the most used algorithm
  - Standard approved by US National Bureau of Standards for Commercial and nonclassified US government use in 1993

Data Encryption Standard (DES) Basics



- DES run in reverse to decrypt
- Cracking DES
  - 1997: 140 days
  - 1999: 14 hours
- TripleDES uses DES 3 times in tandem
  - Output from 1 DES is input to next DES

Encryption Algorithm

Summary

Algorithm	Type	Key Size	Features
DES	Block Cipher	56 bits	Most Common, Not strong enough
TripleDES	Block Cipher	168 bits (112 effective)	Modification of DES, Adequate Security
Blowfish	Block Cipher	Variable (Up to 448 bits)	Excellent Security
AES	Block Cipher	Variable (128, 192, or 256 bits)	Replacement for DES, Excellent Security
RC4	Stream Cipher	Variable (40 or 128 bits)	Fast Stream Cipher, Used in most SSL implementations

Symmetric Encryption

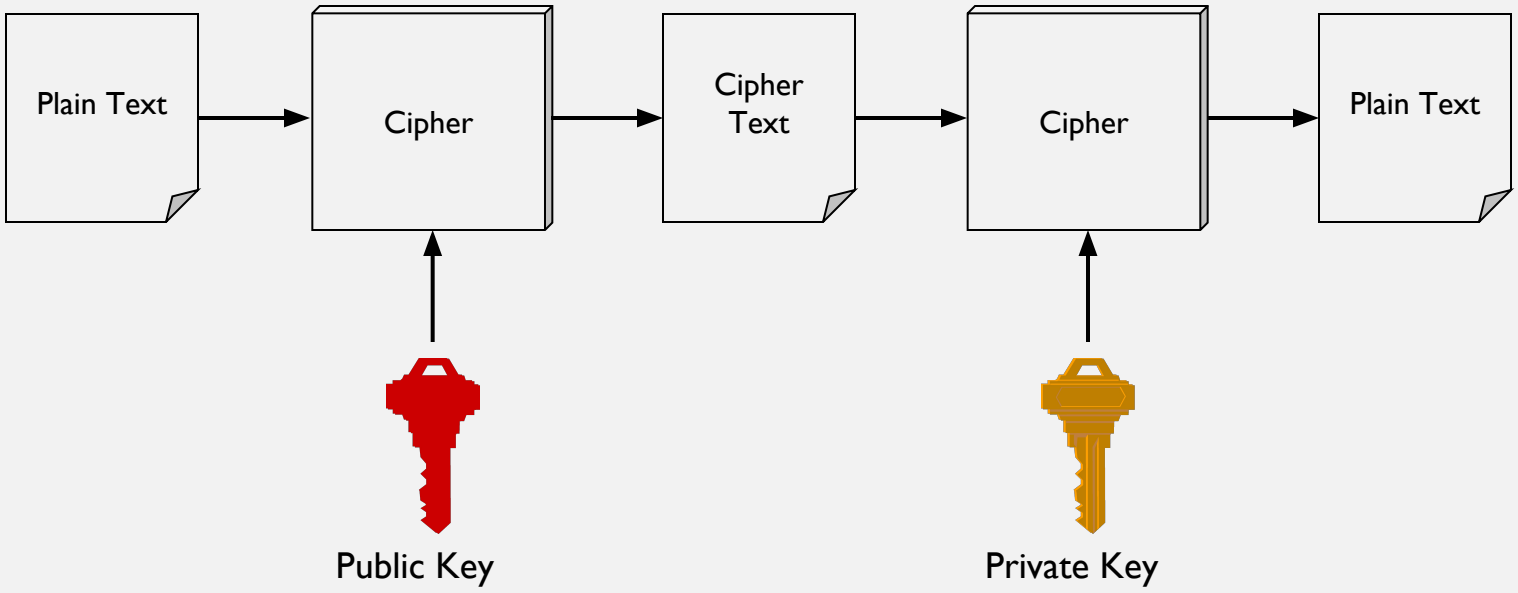
Limitations

- Any exposure to the secret key compromises secrecy of ciphertext
- A key needs to be delivered to the recipient of the coded message for it to be deciphered
  - Potential for eavesdropping attack during transmission of key

Asymmetric Encryption

Basics

- Uses a pair of keys for encryption
  - Public key for encryption
  - Private key for decryption
- Messages encoded using public key can only be decoded by the private key
  - Secret transmission of key for decryption is not required
  - Every entity can generate a key pair and release its public key



Asymmetric Encryption

Types

- Two most popular algorithms are RSA & El Gamal
  - RSA
    - Developed by Ron Rivest, Adi Shamir, Len Adelman
    - Both public and private key are interchangable
    - Variable Key Size (512, 1024, or 2048 buts)
    - Most popular public key algorithm
  - El Gamal
    - Developed by Taher ElGamal
    - Variable key size (512 or 1024 bits)
    - Less common than RSA, used in protocols like PGP

Asymmetric Encryption

RSA

- Choose two large prime numbers p & q
- Compute n=pq and z=(p-1)(q-1)
- Choose number e, less than n, which has no common factor (other than 1) with z
- Find number d, such that ed – 1 is exactly divisible by z
- Keys are generated using n, d, e
  - Public key is (n,e)
  - Private key is (n, d)
- Encryption: $c = m^e \bmod n$
  - m is plain text
  - c is cipher text
- Decryption: $m = c^d \bmod n$
- Public key is shared and the private key is hidden

Asymmetric Encryption

RSA

- P=5 & q=7
- n=5*7=35 and z=(4)*(6) = 24
- e = 5
- d = 29 , (29x5 –1) is exactly divisible by 24
- Keys generated are
  - Public key: (35,5)
  - Private key is (35, 29)
- Encrypt the word love using ($c = m^e \bmod n$)
  - Assume that the alphabets are between 1 & 26

Plain Text	Numeric Representation	m^e	Cipher Text ($c = m^e \bmod n$)
l	12	248832	17
o	15	759375	15
v	22	5153632	22
e	5	3125	10

Asymmetric Encryption

RSA

- Decrypt the word love using ($m = c^d \bmod n$)
  - n = 35, c=29

Cipher Text	c^d	($m = m^e \bmod n$)	Plain Text
17	481968572106750915091411825223072000	17	l
15	12783403948858939111232757568359400	15	o
22	852643319086537701956194499721110000000	22	v
10	100000000000000000000000000000	10	e

Asymmetric Encryption

Weaknesses

- Efficiency is lower than Symmetric Algorithms
  - A 1024-bit asymmetric key is equivalent to 128-bit symmetric key
- Potential for man-in-the middle attack
- It is problematic to get the key pair generated for the encryption

Asymmetric Encryption

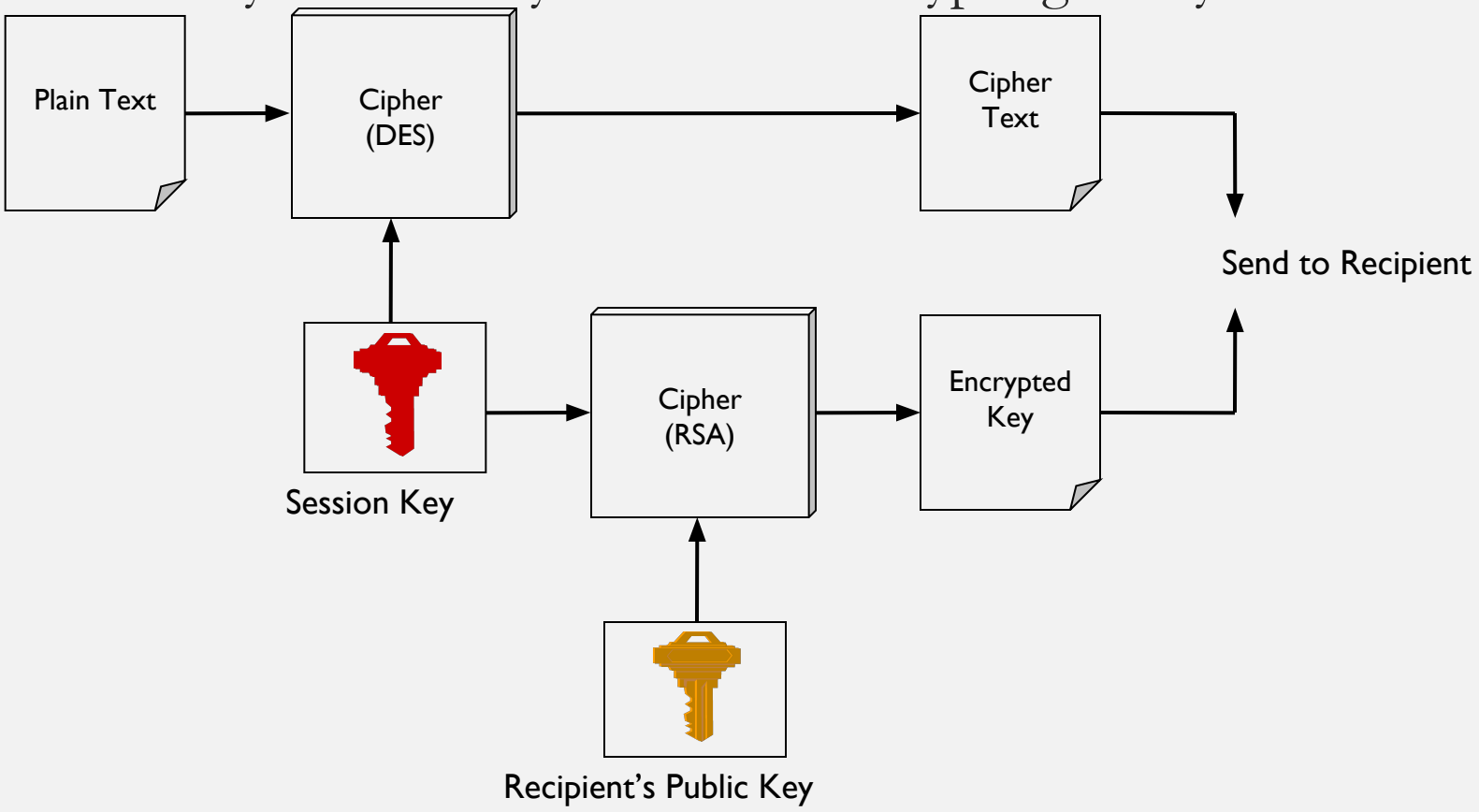
Man-in-the-middle Attack

- Hacker could generate a key pair, give the public key away and tell everybody, that it belongs to somebody else. Now, everyone believing it will use this key for encryption, resulting in the hacker being able to read the messages.

Asymmetric Encryption

Session-Key Encryption

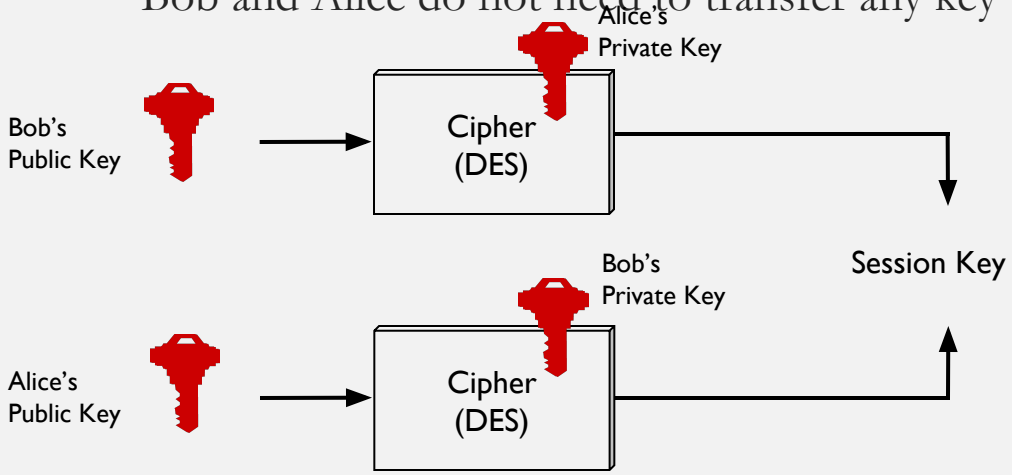
- Used to improve efficiency
  - Symmetric key is used for encrypting data
  - Asymmetric key is used for encrypting the symmetric key



Asymmetric Encryption

Key Agreement

- Key agreement is a method to create secret key by exchanging only public keys.
- Example
  - Bob sends Alice his public key
  - Alice sends Bob her public key
  - Bob uses Alice's public key and his private key to generate a session key
  - Alice uses Bob's public key and her private key to generate a session key
  - Using a key agreement algorithm both will generate same key
  - Bob and Alice do not need to transfer any key



Alice and Bob Generate Same Session Key!

Authentication

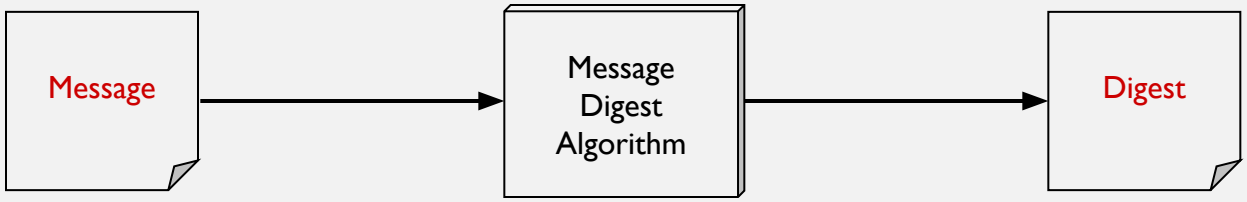
Basics

- Authentication is the process of validating the identity of a user or the integrity of a piece of data.
- There are three technologies that provide authentication
  - Message Digests / Message Authentication Codes
  - Digital Signatures
  - Public Key Infrastructure

Authentication

Message Digests

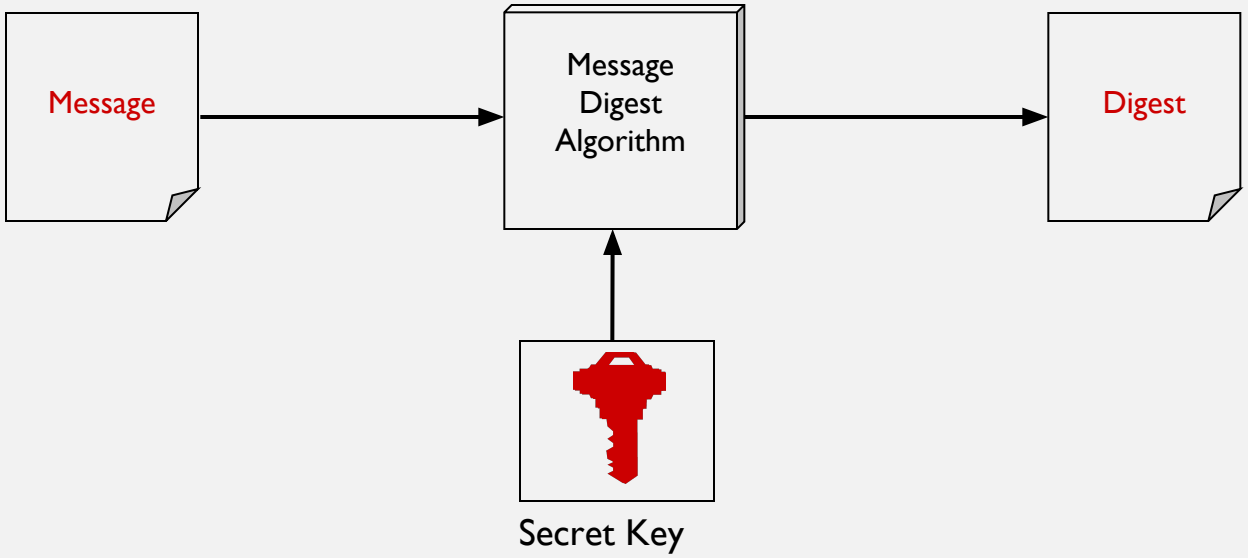
- A message digest is a fingerprint for a document
- Purpose of the message digest is to provide proof that data has not altered
- Process of generating a message digest from data is called hashing
- Hash functions are one way functions with following properties
  - Infeasible to reverse the function
  - Infeasible to construct two messages which hash to same digest
- Commonly used hash algorithms are
  - MD5 – 128 bit hashing algorithm.
  - SHA & SHA-1 – 162 bit hashing algorithm.



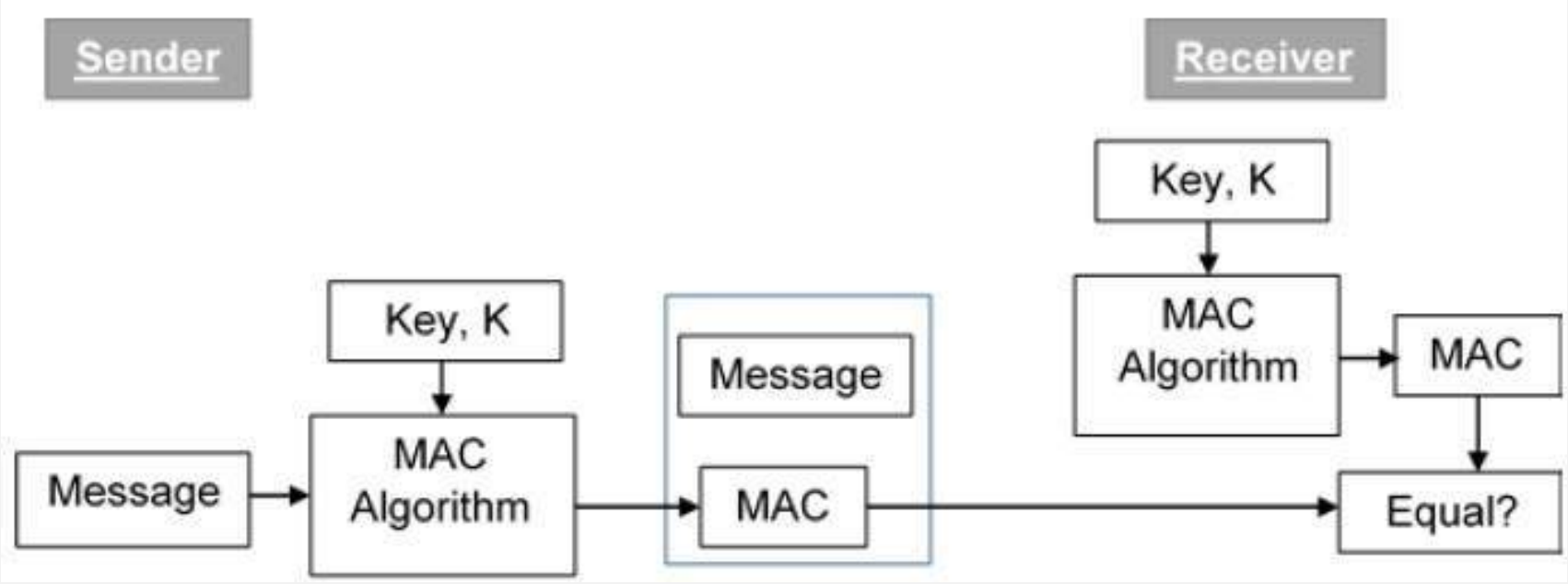
Message Authentication Codes

Basics

- A message digest created with a key
- Creates security by requiring a secret key to be possessed by both parties in order to retrieve the message



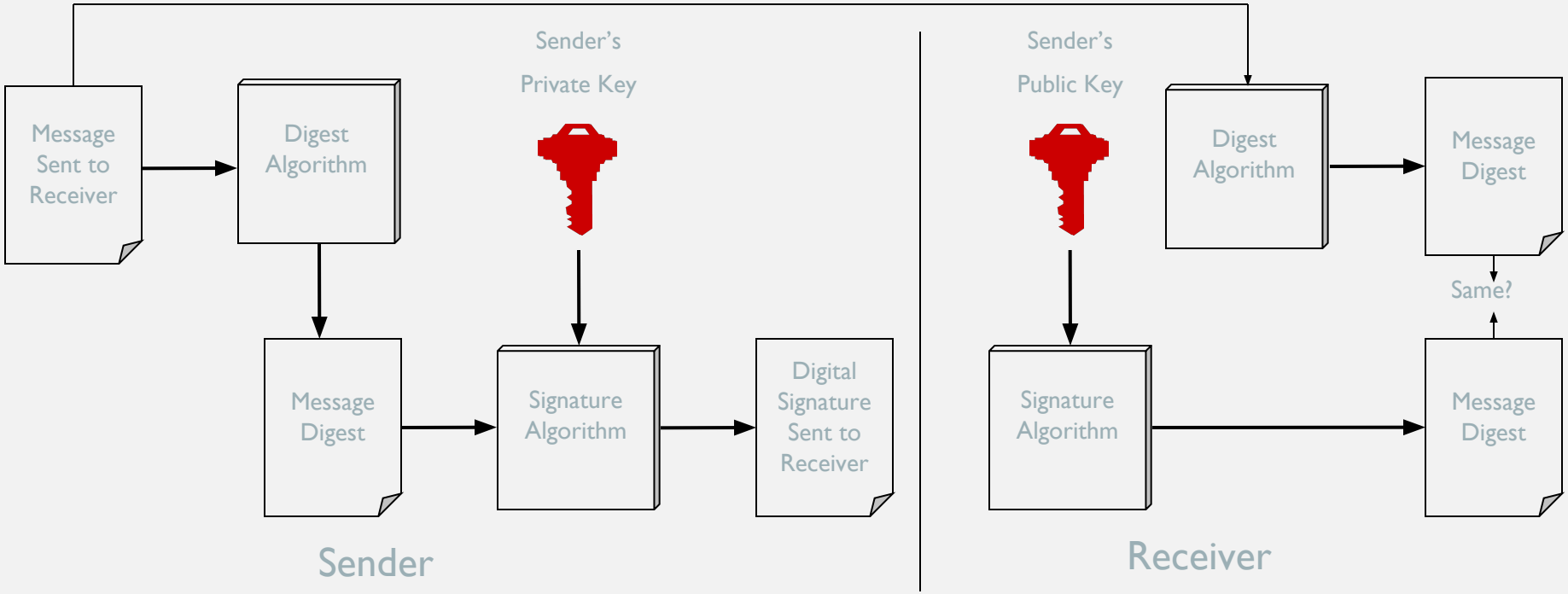
Message Authentication Codes

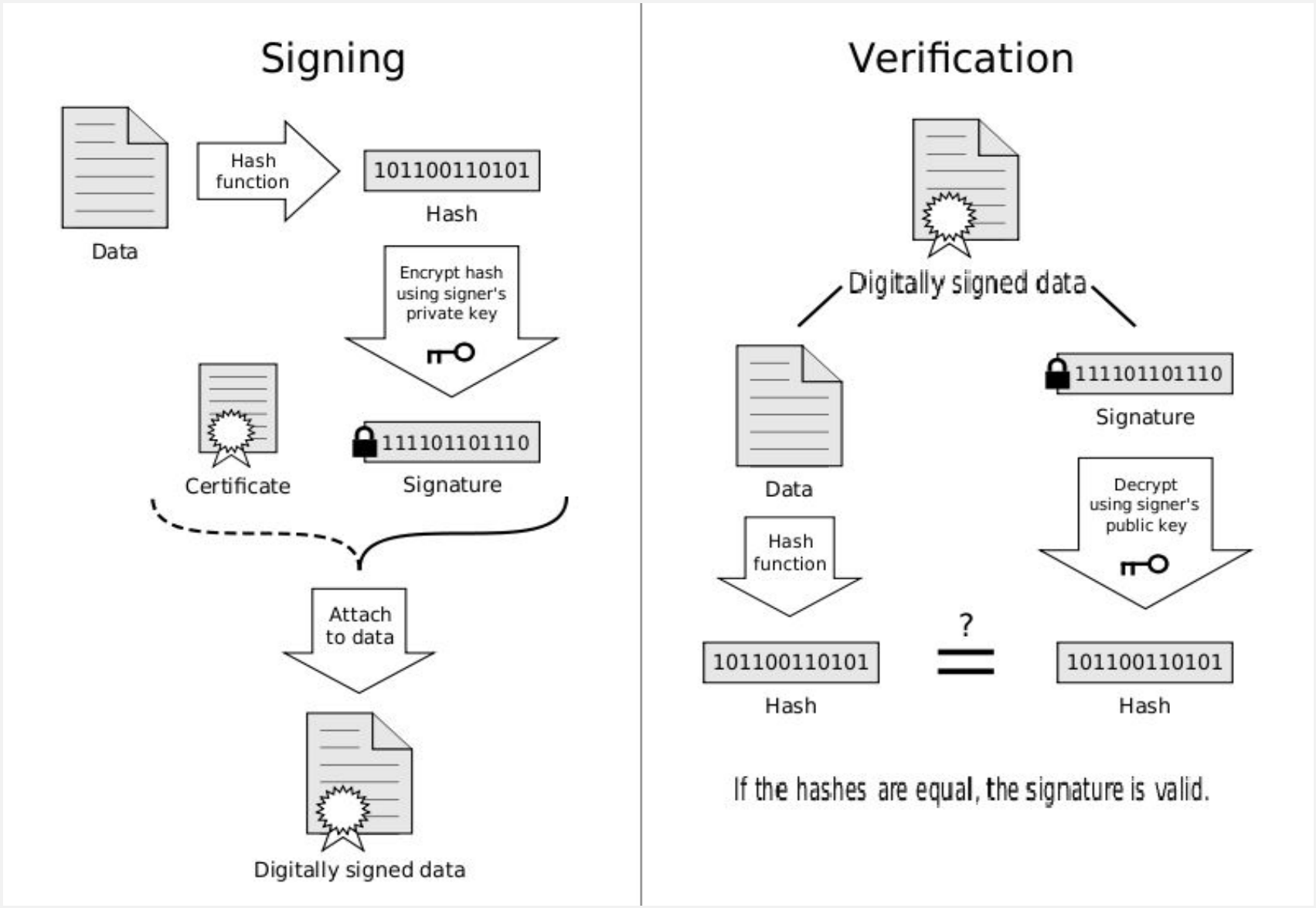


Authentication

Digital Signatures

- A digital signature is a data item which accompanies or is logically associated with a digitally encoded message.
- It has two goals
  - A guarantee of the source of the data
  - Proof that the data has not been tampered with




Signing
Data
Hash function
101100110101
Hash
Encrypt hash using signer's private key
Certificate
111101101110
Signature
Attach to data
Digitally signed data
Verification
Digitally signed data
Data
111101101110
Signature
Decrypt using signer's public key
Hash function
?
101100110101
Hash
101100110101
Hash
If the hashes are equal, the signature is valid.

AT SENDER SIDE

- 1. Message digest is generated using a set of Hash functions.
- 2. A message digest is encrypted using senders private key.
- 3. The resulting encrypted message is known as digital signature.
- 4. Digital signature is attached with data or message and send to receiver.

AT RECEIVER SIDE

1. Receiver uses senders public key to decrypt senders digital signature to obtain message digest send by receiver.

2. Receiver uses same message digest algorithm, which is used by sender

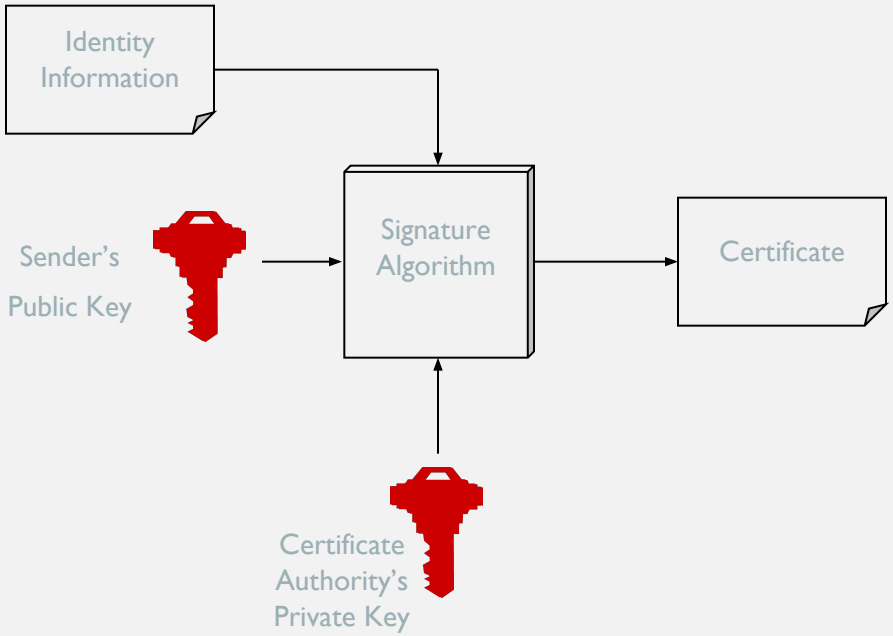
3. Now, receiver will compare these two message digest

4. If message digest are equal then signature is valid else not.

Authentication

Digital Cerftificates

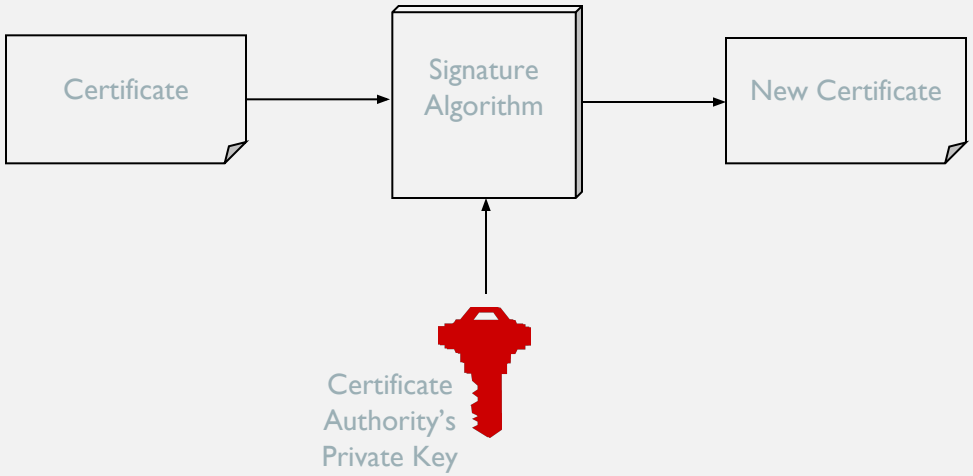
- A digital certificate is a signed statement by a trusted party that another party's public key belongs to them.
  - This allows one certificate authority to be authorized by a different authority (root CA)
- Top level certificate must be self signed
- Any one can start a certificate authority
  - Name recognition is key to some one recognizing a certificate authority
  - Verisign is industry standard certificate authority



Authentication

Cerftificates Chaining

- Chaining is the practice of signing a certificate with another private key that has a certificate for its public key.
  - Similar to the passport having the seal of the government
- It is essentially a person's public key & some identifying information signed by an authority's private key verifying the person's identity.
- The authorities public key can be used to decipher the certificate.
- The trusted party is called the certificate authority.



Applications of Cryptography

- Digital currency
- E-commerce
- Military operations
- Secure Communication

FIREWALLS

INTRODUCTION

- Firewalls control the flow of network traffic
- Firewalls have applicability in networks where there is no internet connectivity
- Firewalls operate on number of layers
- Can also act as VPN gateways
- Active content filtering technologies

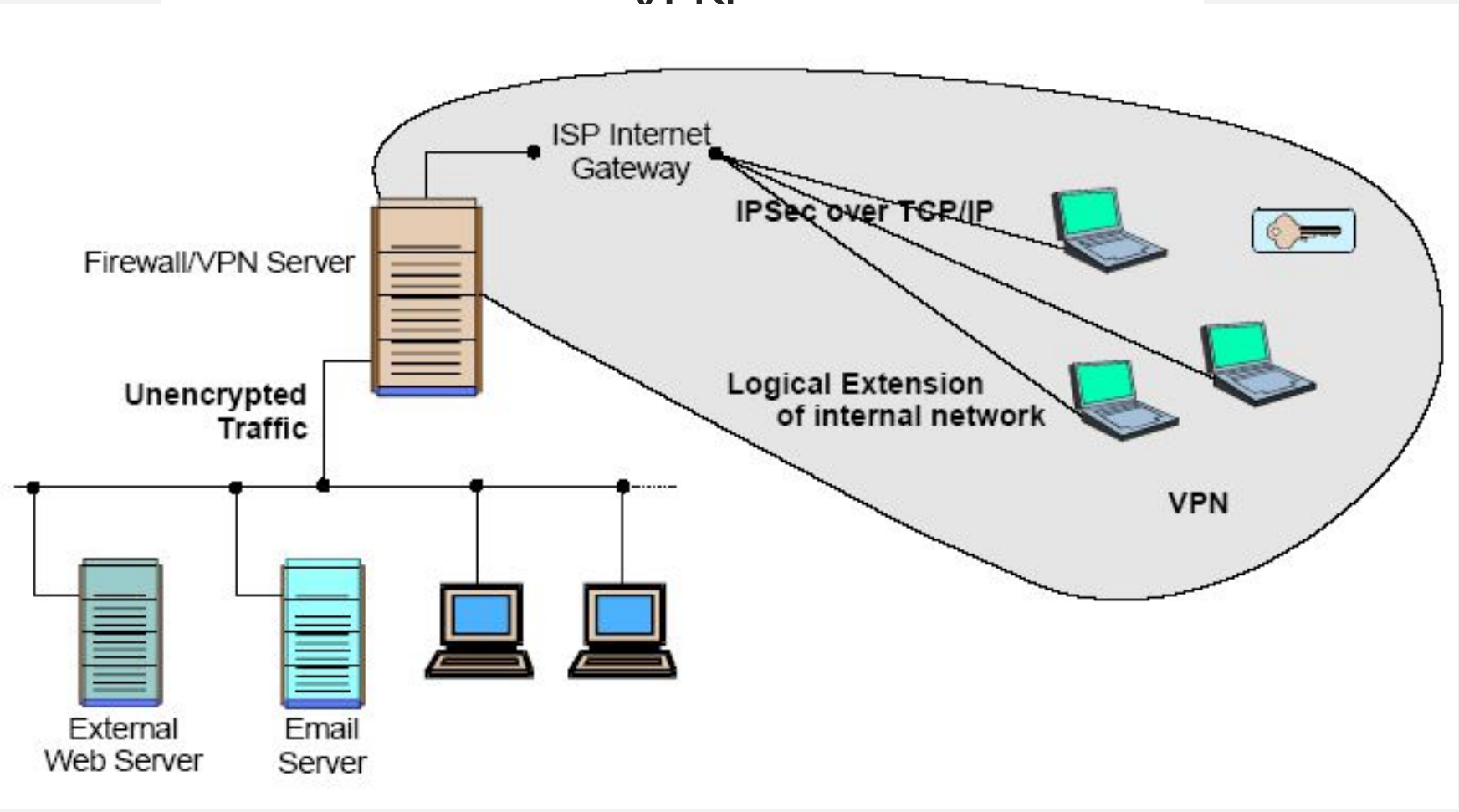
FIREWALL ENVIRONMENTS

- There are different types of environments where a firewall can be implemented.
- Simple environment can be a packet filter firewall
- Complex environments can be several firewalls and proxies

VPN

- VPN is used to provide secure network links across networks
- VPN is constructed on top of existing network media and protocols
- On protocol level IPsec is the first choice
- Other protocols are PPTP, L2TP

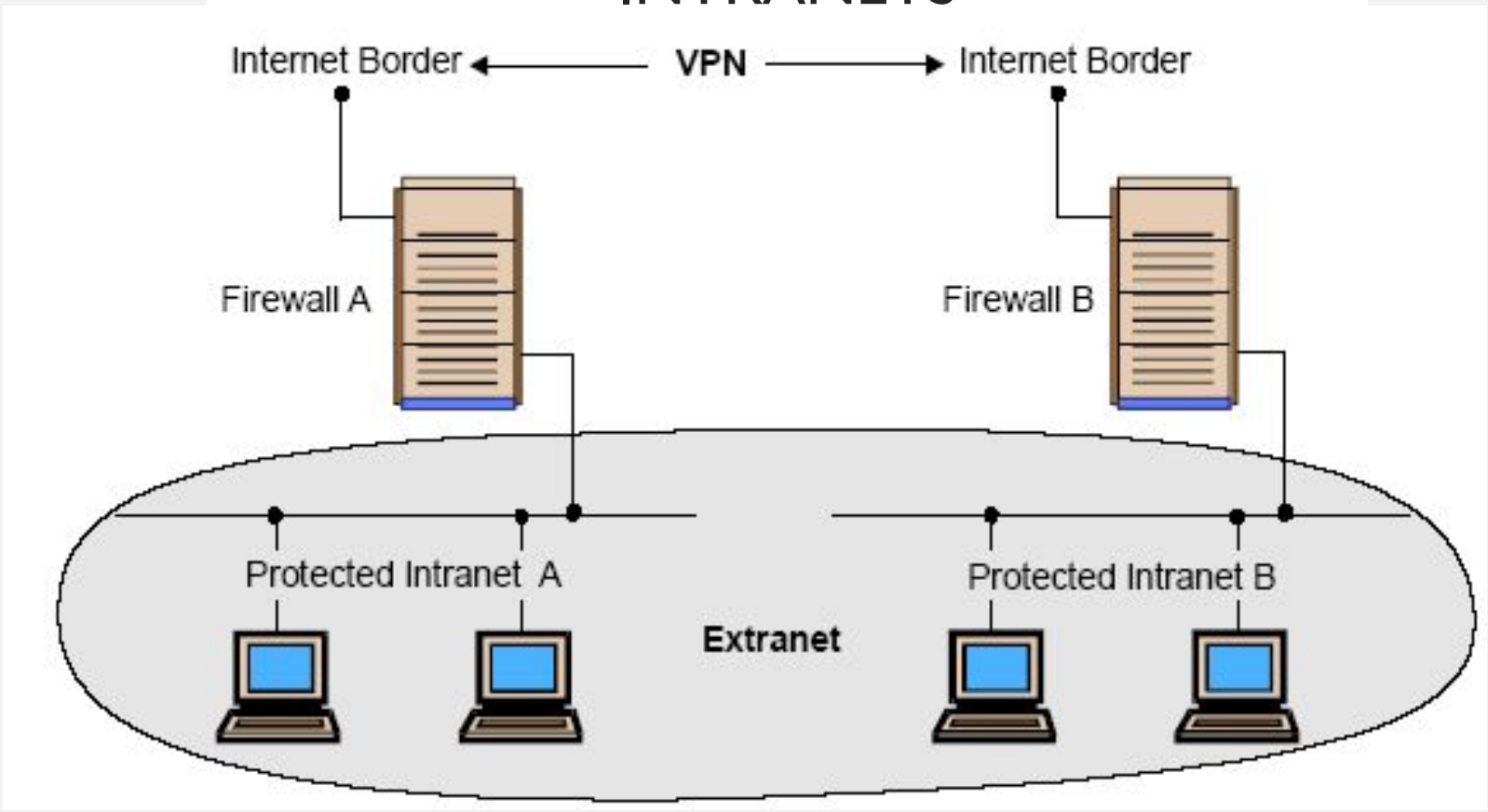
VPN


ISP Internet
Gateway
IPSec over TCP/IP
Firewall/VPN Server
Unencrypted
Traffic
Logical Extension
of internal network
VPN
External
Web Server
Email
Server

INTRANETS

- An intranet is a network that employs the same types of services, applications, and protocols present in an Internet implementation, without involving external connectivity
- Intranets are typically implemented behind firewall environments.

INTRANETS


Internet Border
VPN
Internet Border
Firewall A
Firewall B
Protected Intranet A
Protected Intranet B
Extranet

EXTRANETS

- Extranet is usually a business-to-business intranet
- Controlled access to remote users via some form of authentication and encryption such as provided by a VPN
- Extranets employ TCP/IP protocols, along with the same standard applications and services

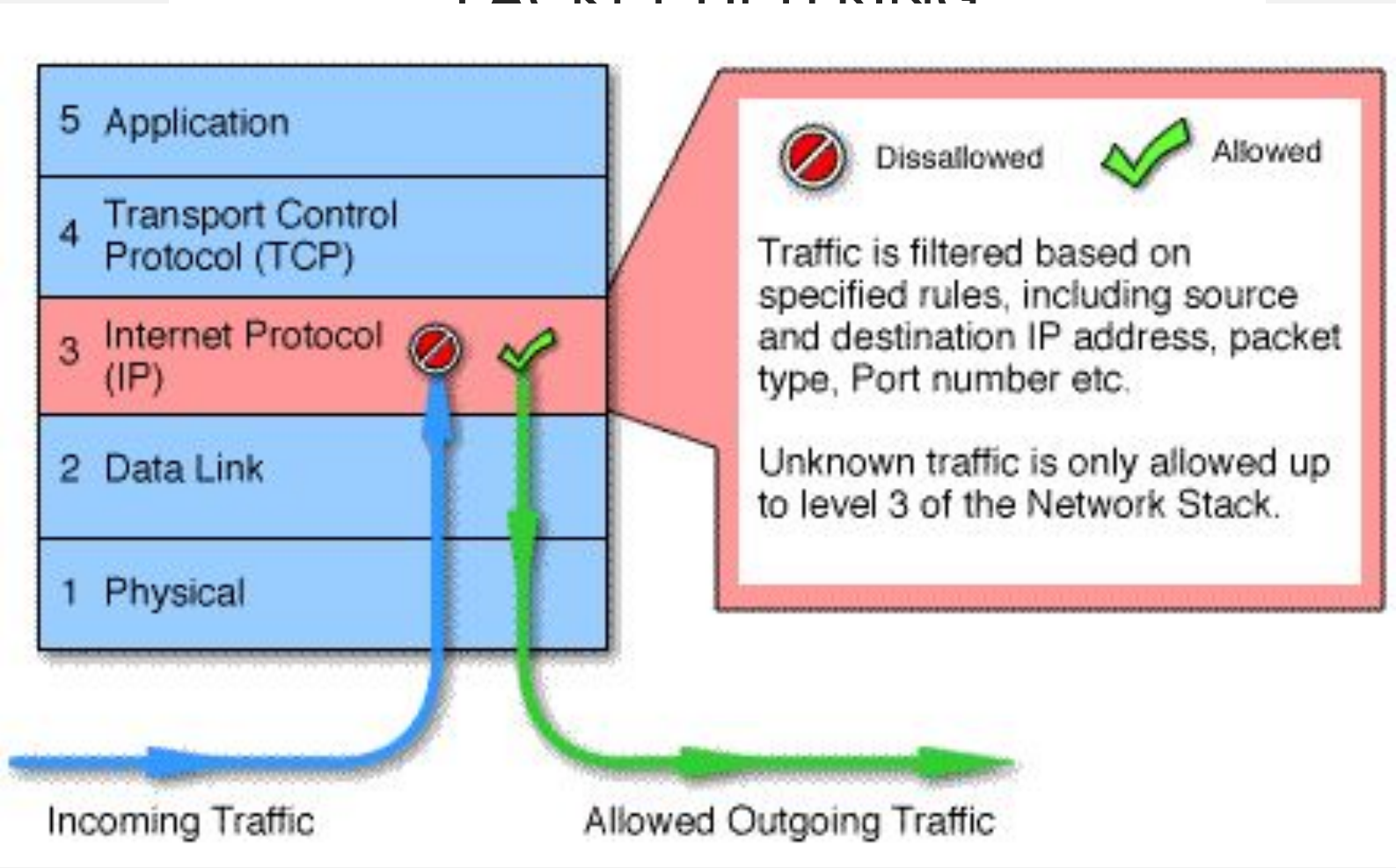
TYPES OF FIREWALLS

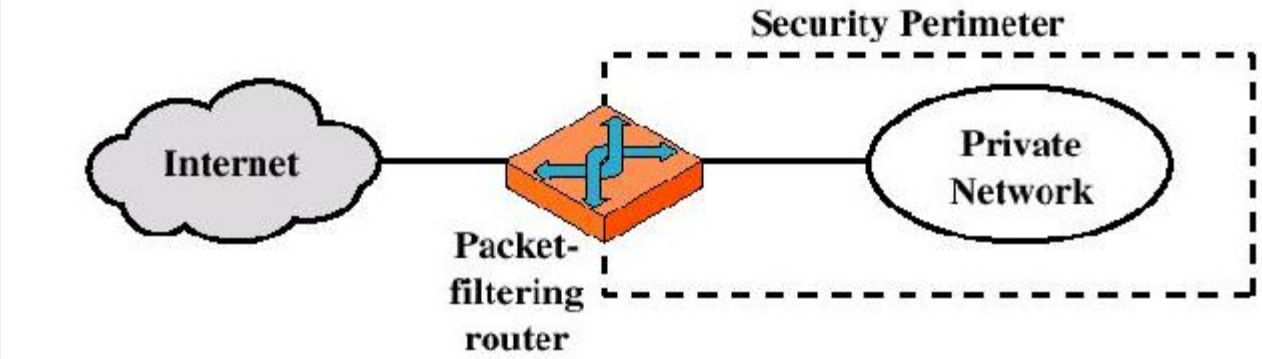
- Firewalls fall into four broad categories
  - Packet filters
  - Circuit level
  - Application level
  - Stateful multilayer

PACKET FILTER

- Works at the network level of the OSI model
- Each packet is compared to a set of criteria before it is forwarded
- Packet filtering firewalls is low cost and low impact on network performance

PACKET FILTERING




Security Perimeter
Internet
Private
Network
Packet-
filtering
router

- Packet-filtering Router
  - Applies a set of rules to each incoming IP packet and then forwards or discards the packet
  - Filter packets going in both directions
  - The packet filter is typically set up as a list of rules based on matches to fields in the IP or TCP header
  - Two default policies (discard or forward)

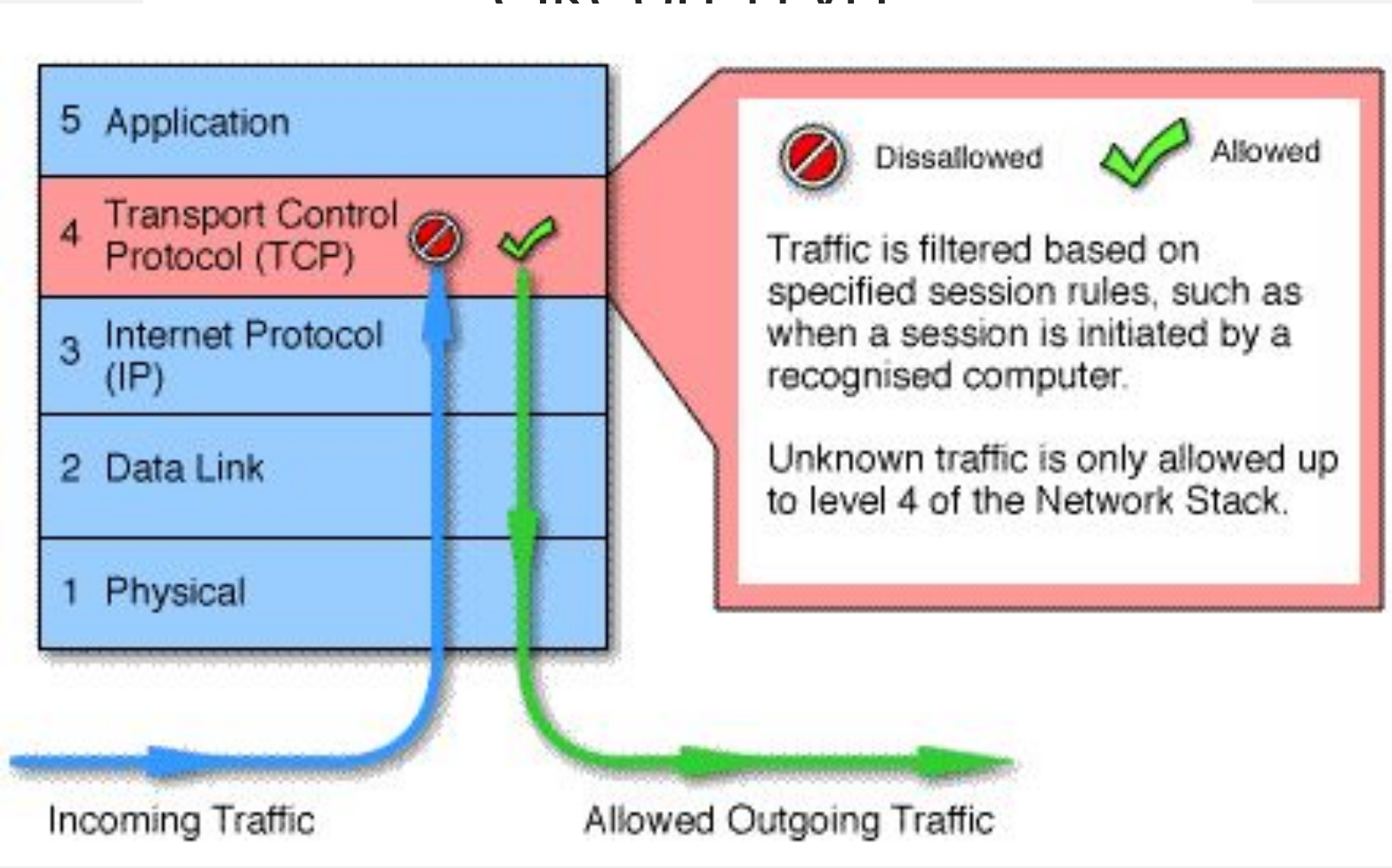
- Advantages:
  - Simplicity
  - Transparency to users
  - High speed
- Disadvantages:
  - Difficulty of setting up packet filter rules
  - Lack of Authentication

- Possible attacks
  - IP address spoofing
  - Source routing attacks
  - Tiny fragment attacks

CIRCUIT LEVEL

- Circuit level gateways work at the session layer of the OSI model, or the TCP layer of TCP/IP
- Monitor TCP handshaking between packets to determine whether a requested session is legitimate.
- Specialized function performed by an Application-level Gateway
- Sets up two TCP connections
- The gateway typically relays TCP segments from one connection to the other without examining the contents

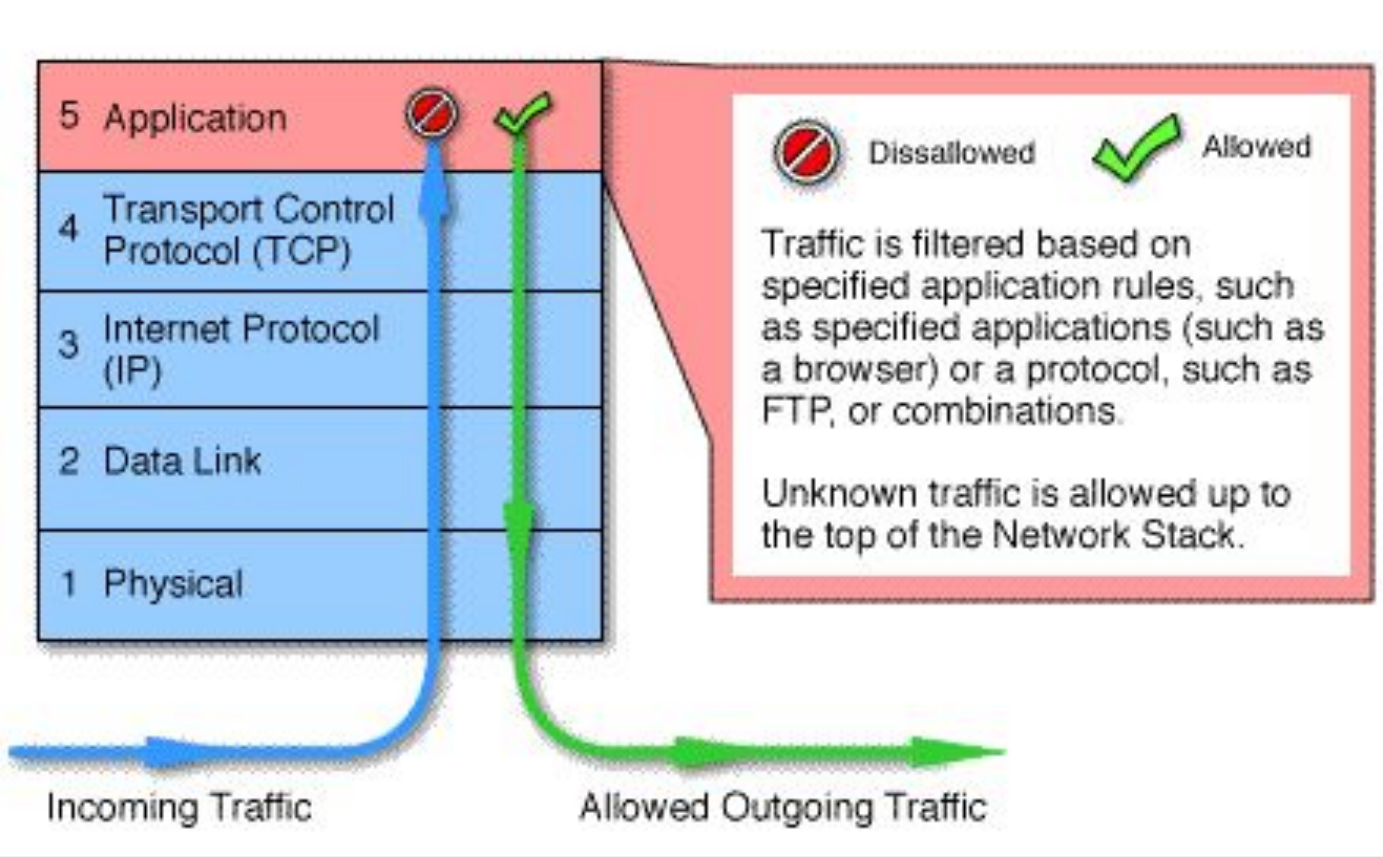
CIRCUIT LEVEL

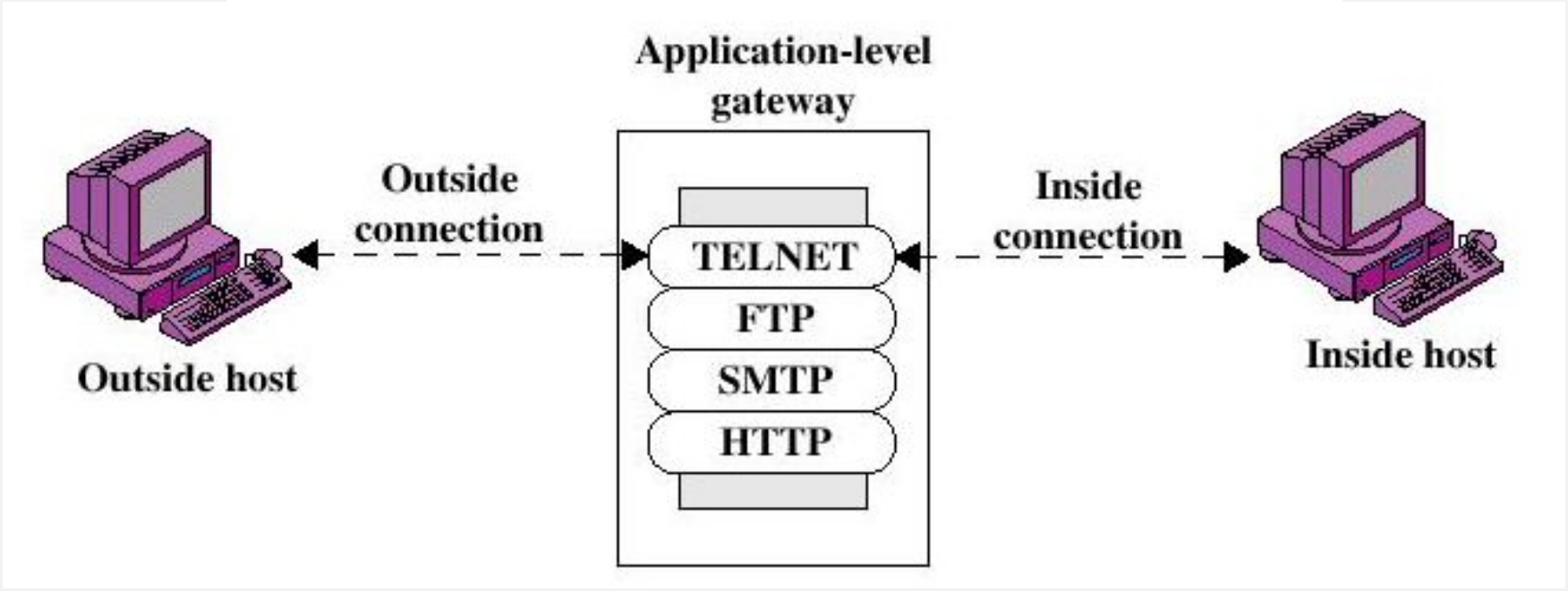


APPLICATION LEVEL

- Application level gateways, also called proxies, are similar to circuit-level gateways except that they are application specific
- Gateway that is configured to be a web proxy will not allow any ftp, gopher, telnet or other traffic through

APPLICATION LEVEL



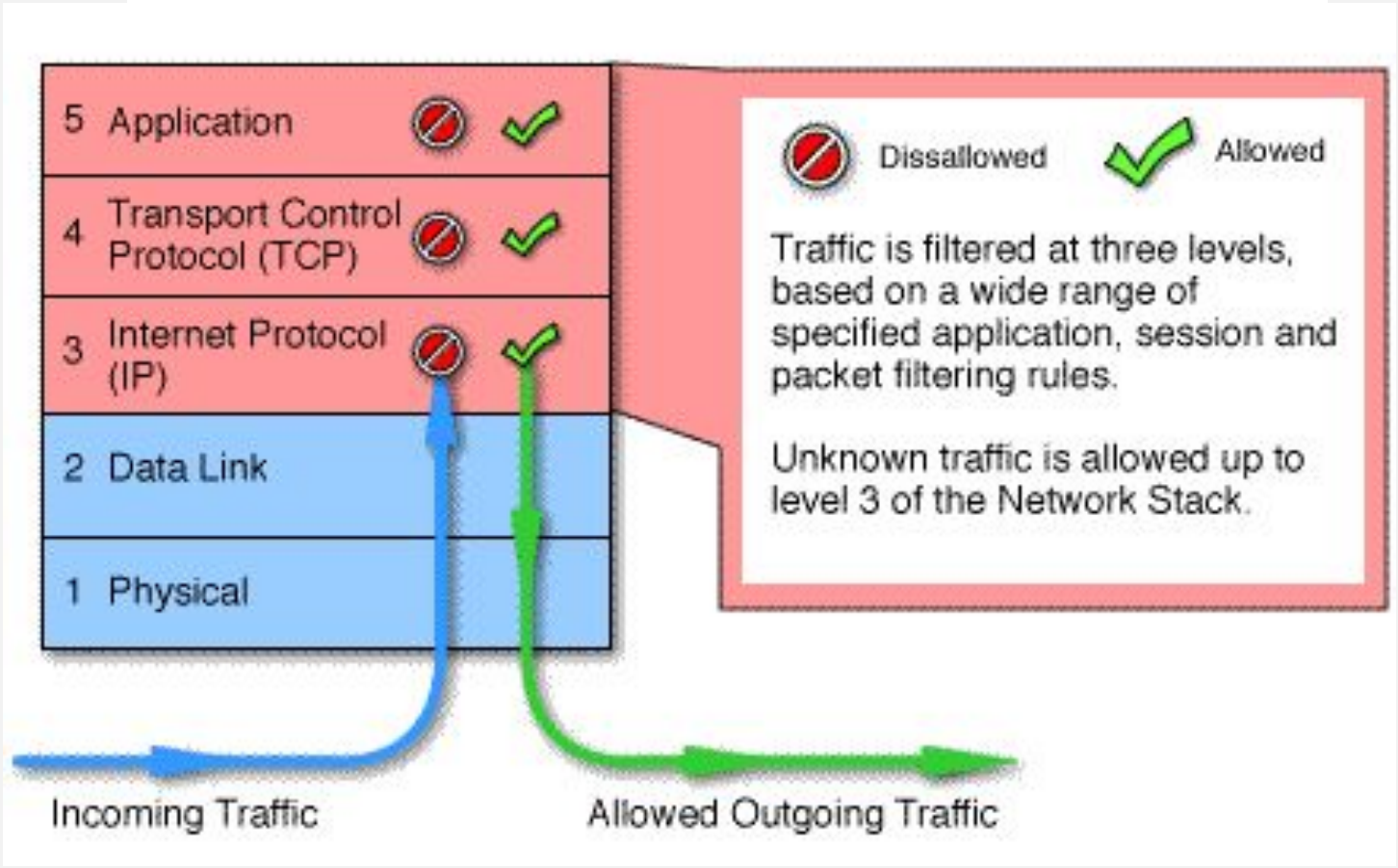

Application-level
gateway
Outside
connection
Inside
connection
TELNET
FTP
SMTP
HTTP
Outside host
Inside host

- Advantages:
  - Higher security than packet filters
  - Only need to scrutinize a few allowable applications
  - Easy to log and audit all incoming traffic
- Disadvantages:
  - Additional processing overhead on each connection (gateway as splice point)

STATEFUL MULTILAYER

- Stateful multilayer inspection firewalls combine the aspects of the other three types of firewalls
- They filter packets at the network layer, determine whether session packets are legitimate and evaluate contents of packets at the application layer

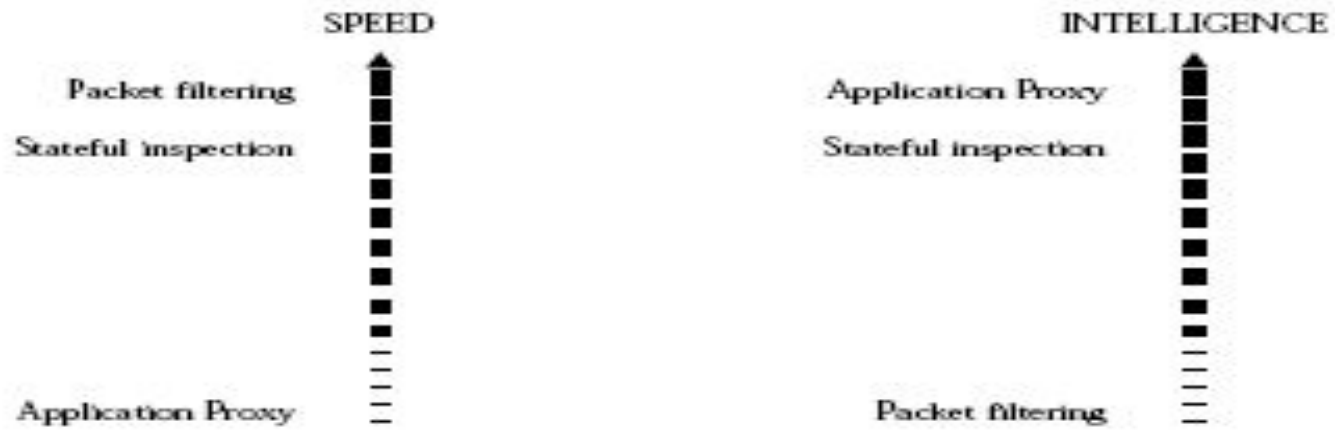
STATEFUL MULTILAYER



GENERAL PERFORMANCE

FIREWALL PERFORMANCE SUMMARY

Technology	Speed	Flexibility	Intelligence
Packet filtering	V. Good	V.Good	Low
Application Proxy	Low	Low	V. Good
Stateful inspection	Good	Good	Good
Circuit gateway	Low	Low	Low



FUTURE OF FIREWALLS

- Firewalls will continue to advance as the attacks on IT infrastructure become more and more sophisticated
- More and more client and server applications are coming with native support for proxied environments
- Firewalls that scan for viruses as they enter the network and several firms are currently exploring this idea, but

CONCLUSION

- It is clear that some form of security for private networks connected to the Internet is essential
- A firewall is an important and necessary part of that security, but cannot be expected to perform all the required security functions.