5 Computer Networks Communications Architecture and Protocols

Part 13

Network Security

Goals of Network Security (1)

- Confidentiality
  - Information is only accessible to the intended party
  - Unknown existence of message also part of confidentiality
- Authentication
  - Sender and receiver need to confirm identity of the other party involved in the communication
- Message Integrity
  - Ensure that the contents of the communication is not altered – either malicious or by accident

Goals of Network Security (2)

- Nonrepudiation
  - Proof of transmission
  - Sender and receiver should be unable to deny transmission
- Access control – Authorisation
  - Only authorized people should have access to a target system
- Availability
  - System should be up and running
  - Data is available to authorized parties

Security Threats

- Passive Threats
  - Release of message contents
  - Traffic analysis
- Active Threats
  - Masquerade
  - Replay
  - Modification of message contents
  - Denial of service

Passive Attacks

- Eavesdropping on transmissions
  - Goal is to obtain information
- Release of message contents
  - Outsider learns content of transmission
- Traffic analysis
  - By monitoring frequency and length of messages, even encrypted, nature of communication may be guessed
- Difficult to detect
  - Does not involve any alteration to data
- Can be prevented
  - E.g. masking contents by using encryption

Active Attacks (1)

- Masquerade
  - Pretending to be a different entity
  - Usually includes another active attack
- Replay
  - Involves passive capture of data units
  - Retransmitted to produce an unauthorised effect
- Modification of messages
  - Legitimate message is altered, delayed or reordered to produce an unauthorised effect

Active Attacks

- Denial of service attacks
  - Prevents the network form providing normal services
  - E.g flooding the network with messages (SYN flooding) ➔ over consuming resources
  - Routing tables modifications
- Easy to detect
  - Detection may lead to deterrent
- Hard to prevent

Defense (1)

- Threat monitoring
  - Check for suspicious patterns of activity
- Audit logs
  - Record the time, user and all accesses to objects by users
  - Log files can become very large – opt to scan system periodically

Defense (2)

- Passwords – have good password policy
  - Expire passwords after a time, require change
  - Lock after repeated attempts
  - Logon procedures
  - Restrict logon only from certain hosts
  - Minimum password lengths
- Encryption - make message or data undecipherable ; see later

Defense (3)

- Packet filtering
  - Can be based on source and destination IP addresses and Port numbers
    - E.g. restrict HTTP connections to specific list of public web servers
    - E.g. deny all network from a specific host or network
  - ICMP message types and TCP SYN or ACK
    - Only reply ICMP messages are allowed
    - Prevents e.g. external clients form making TCP connections with internal hosts

Defense (4)

- Firewalls
  - Replaces IP router with multihomed host that does not forward *all* packets.
  - Acts as an application gateway
- Host authentication – confirm that host is the intended one
- User authentication
  - Confirm that user is the right one
- Key authentication
  - Session keys are commonly to indicate a communication rendezvous between parties willing to communicate.

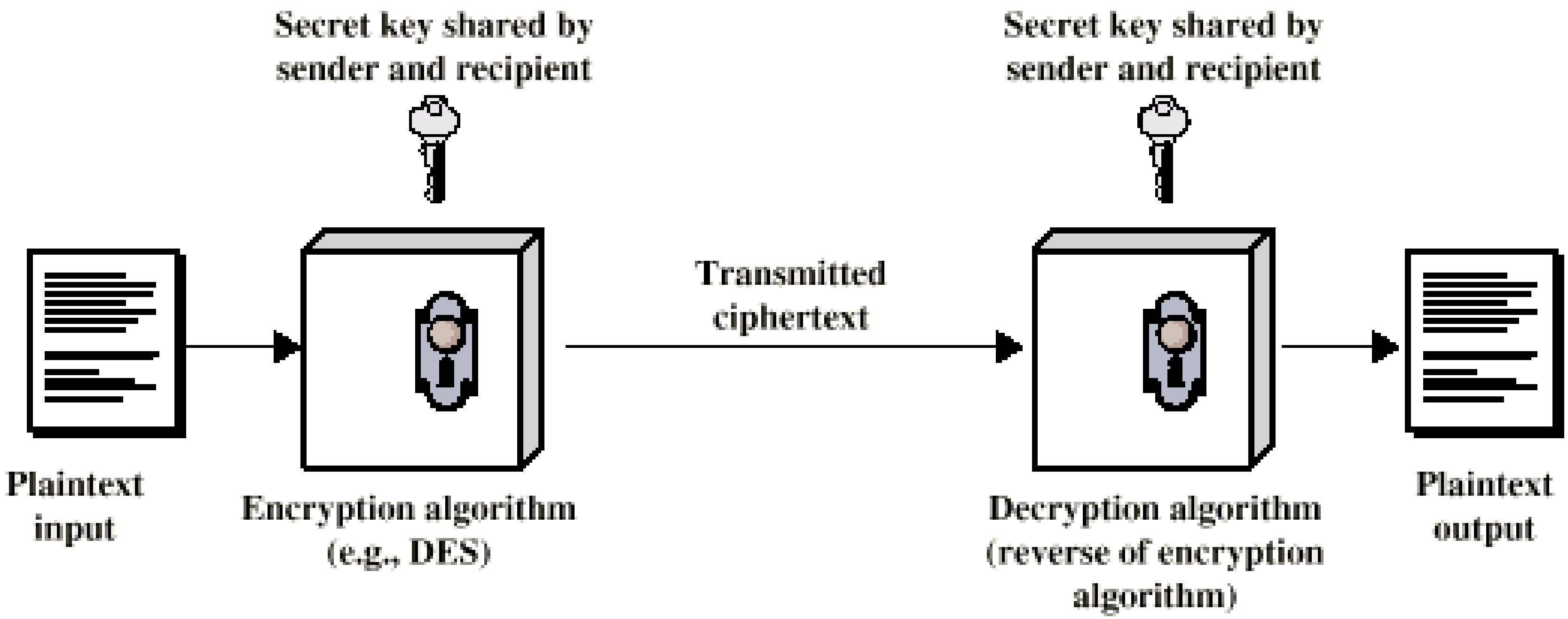
Firewalls

- Common hardware approach to network security
- Types of firewalls include filtering at level 2 (frames) and level 3 (packets)
- Monitor all transactions between two systems

Components

- Plain text (m)
  - Original data or message that is fed into the algorithm
- Encryption algorithm (E)
  - Performs substitutions and transformations to the plaintext
- Secret key (K)
  - Determines the exact substitutions and transformations in the encryption algorithm
- Cipher text
  - Scrambled message produced as output
- Decryption algorithm (D)
  - Takes the cyphertext and the secret key to produce the original plaintext

Conventional Encryption



Requirements for Security

- Strong encryption algorithm
  - Even if known, should not be able to decrypt or work out key
  - Even if a number of cipher texts are available together with plain texts of them
- Sender and receiver must obtain secret key securely
- Once key is known, all communication using this key is readable

Attacking Encryption

- Crypt analysis
  - Relay on nature of algorithm plus some knowledge of general characteristics of plain text
  - Attempt to deduce plain text or key
- Brute force
  - Try every possible key until plain text is achieved

Basic Techniques (1)

- Substitution
  - take each letter in plaintext message and substitute letter which is k letters later,I.e. k is the key(eg. K=4)

Plaintext alphabet:	a	b	c	d	e	f	g	h	i	j	k	l	…
Ciphertext alphabet:	e	f	g	h	i	j	k	l	m	n	o	p	…
Plaintext:	I		L	O	V	E		Y	O	U			
Ciphertext:	M		P	S	Z	I		C	S	Y			

Basic Techniques (2)

Randomised substitution – monoalphabetic cipher

Plaintext alphabet:	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
Ciphertext alphabet:	z	h	x	k	m	p	f	a	w	t	u	b	y
	g	c	v	d	n	j	l	e	i	o	q	r	s
Plaintext:	I		L	O	V	E		Y	O	U			
Ciphertext:	W		B	C	I	M		R	C	E			

Basic Techniques (2)

- Transposition – use a key to reorder the plaintext characters in groups based on column

Q	U	I	C	K	S	A	N	D	<- Key
7	9	4	2	5	8	1	6	3	
p	l	e	a	s	e	-	s	e	
n	d	-	m	e	-	a	-	m	
i	l	l	i	o	n	-	r	a	
n	d	-	a	s	-	s	o	o	
n	-	a	s	-	p	o	s	s	
i	b	l	e	-	-	-	-	-	

The plaintext is: please send me a million rand as soon as possible

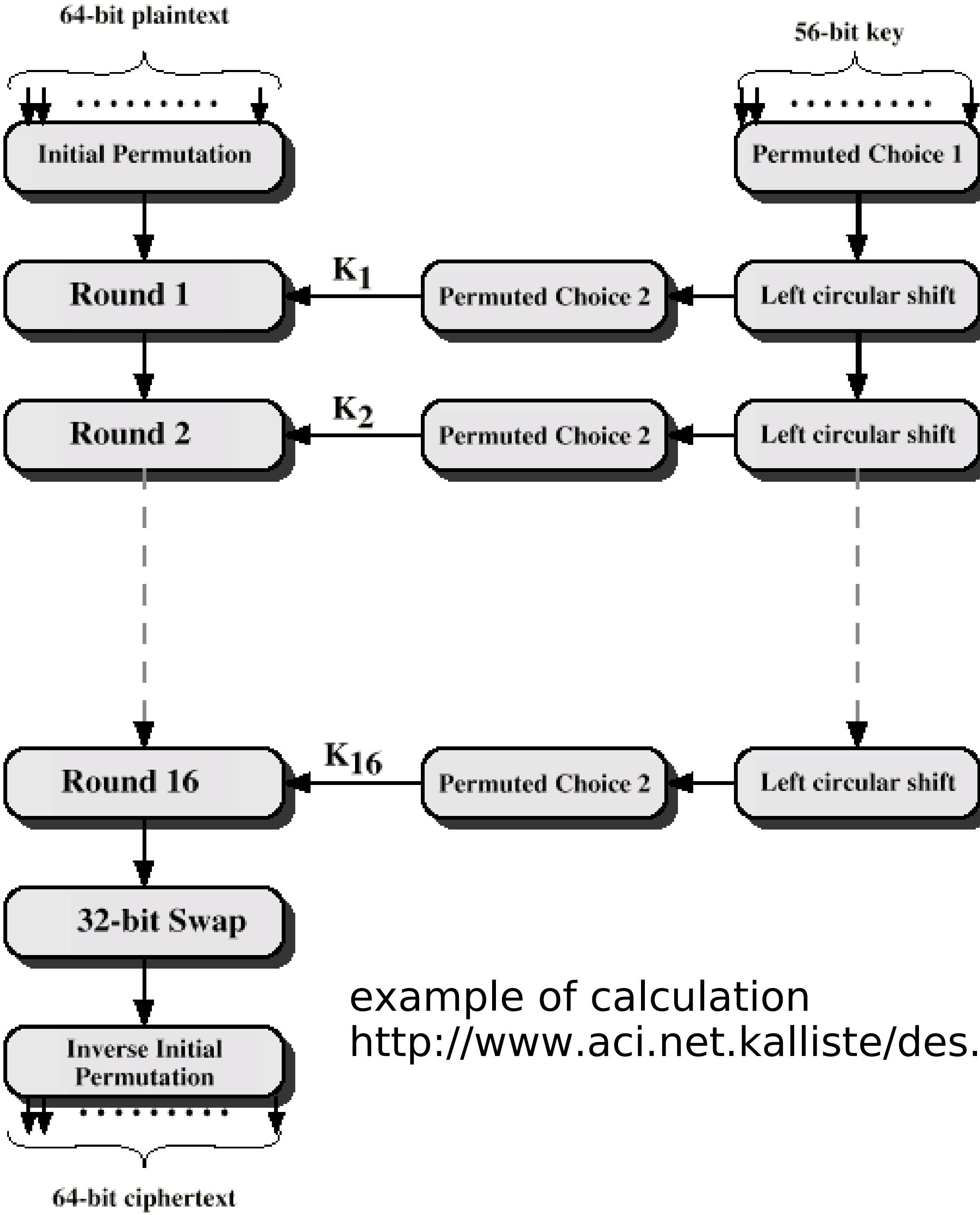
Data Encryption Standard (1) (DES)

- A symmetric–key encryption standard
  - Also called a private key cryptosystem
  - Published in 1977 and updated in1993 by the NBS (now NIS) for commercial and non-classified US Gov. use

Data Encryption Standard (2) (DES)

- A Block cipher
  - Processes plain text in fixed block sizes of 64-bits producing block of cipher text of equal size
  - Uses 64-bit key –
    - 8 bits of the 64 bits are for odd parity ➔ every 8^{th} bit in the key is not used
    - DES key is effectively 56 bits.
- Operation
  - Two permutation steps (first and last)
  - 16 identical rounds of operations in between

DES Encryption Algorithm

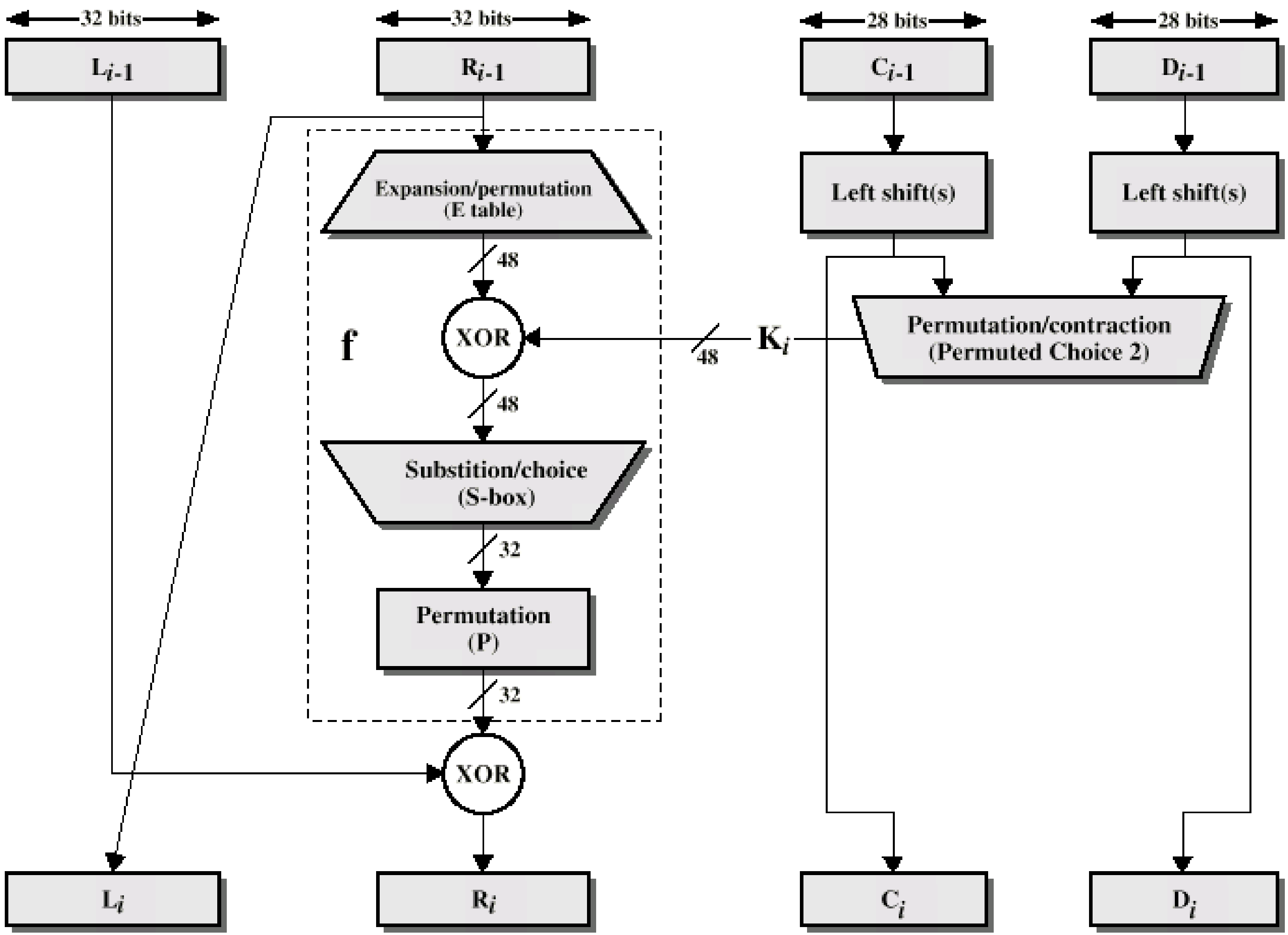


example of calculation
http://www.aci.net.kalliste/des.htm

DES Single Iteration

$L_i = R_{i-1}$

$R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$



Strength of DES (1)

- In 1997 RSA Data security Inc. launched a DES challenge contest
  - Crack a short phrase encrypted using 56-bit DES
  - "Strong cryptography makes the work a safer place"
  - Cracked in about four months after trying out 18 quadrillion keys – a quarter of the search space. Claimed US$ 10,000.

Strength of DES (2)

- 1998 DES challenge III cracked in about 22 hours by Electronic Frontier Foundation using a DES cracker machine. Scooped US$250,000
- DES declared insecure in 1998
- DES now worthless

Triple DES

- Run 56-bit algorithm multiple times
  - Take 64-bit output from one iteration as input to next DES iteration
  - Use different encryption key each time
- Triple DES is proposed standard (1999)
- Uses 3 keys and 3 executions of DES algorithm
- Effective key length 168 bit

Link Encryption

- With link encryption each communication link is equipped at both ends with an encryption device
- All traffic secure
- High level of security
- Requires lots of encryption devices
- Message must be decrypted at each switch to read address (virtual circuit number)
- Security vulnerable at switches
  - Particularly on public switched network

End to End Encryption

- Encryption done at ends of system
- Data in encrypted form crosses network unaltered
- Destination shares key with source to decrypt
- Host can only encrypt user data
  - Otherwise switching nodes could not read header or route packet
- Traffic pattern not secure
- → Use both link and end to end

Key Distribution

- Key selected by A and physically delivered to B
- Third party selects key and physically delivers to A and B
- If A and B recently used a key ➔ use old key to encrypt new key and transmit new key from A to B
- A and B have encrypted connection to third party C ➔ C can deliver key on encrypted links to A and B

Automatic Key Distribution (1)

- Session Key
  - Used for duration of one logical connection
  - Destroyed at end of session
  - Used for user data, all user data are encrypted with a one-session key

Automatic Key Distribution

- Permanent key
  - Used between entities for distributing session keys
  - Key distribution center
    - Determines which systems may communicate with each other
    - When permission is granted ➔ provides one session key for that connection
  - Front end processor
    - Performs end to end encryption
    - Obtains keys for host

Public Key Cryptography

- Private key systems suffer from the key distribution problem
- Use two keys: one public and one private with the following requirements:
  - D(E(P)) = P
  - Very difficult to deduce D from E
  - E cannot be broken by a chosen plaintext attack
- Publish the public key and keep private key secret
- Anyone can send you encrypted messages, but only you can decrypt.

E=encryption algorithm
D=decryption algorithm
P=plaintext

Message Authentication

- Protection against active attacks
  - Falsification of data
  - Eavesdropping
- Message is authentic if it is genuine and comes from the alleged source
- Authentication allows receiver to verify that message is authentic
  - Message has not altered
  - Message is from authentic source
  - Message timeline

Authentication Using Encryption

- Assumes sender and receiver are only entities that know key
- Message includes:
  - error detection code
  - sequence number
  - time stamp

no alterations have been made

Authentication Without Encryption

- Authentication tag generated and appended to each message
- Message not encrypted
- Useful for:
  - Messages broadcast to multiple destinations
    - Have one destination responsible for authentication ➔ cheaper and more reliable
  - One side heavily loaded and cannot afford time to decrpyt
    - Encryption adds to workload
    - Can authenticate random messages
  - Programs authenticated without encryption can be executed without decoding

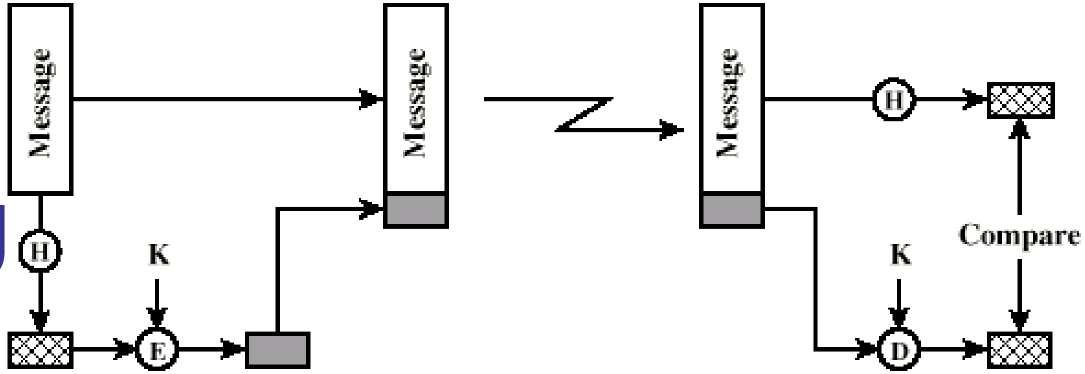
Message Authentication Code

- Generate authentication code based on shared key and message
- Common key shared between A and B
- If only sender and receiver know key and code matches:
  - Receiver assured message has not altered
  - Receiver assured message is from alleged sender
  - If message has sequence number, receiver assured of proper sequence

One Way Hash Function

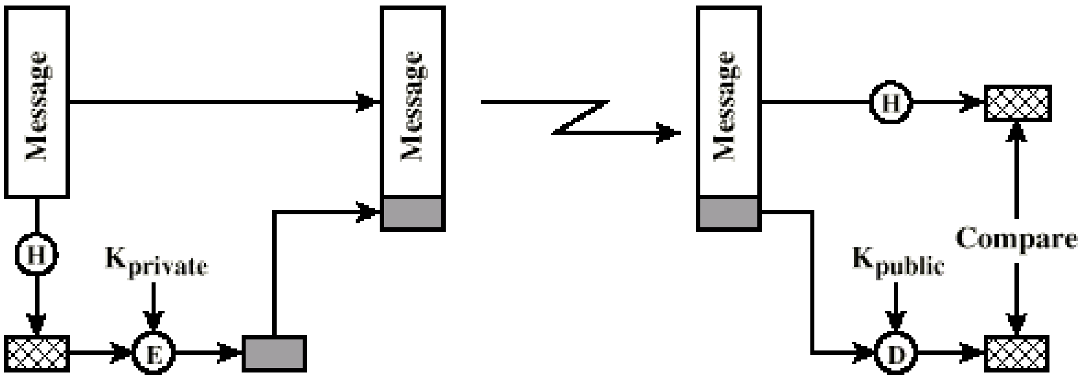
- Variation of message authentication code
- Accepts variable size message and produces fixed size tag (message digest)
- Advantages of authentication without encryption
  - Encryption is slow
  - Encryption hardware expensive
  - Encryption hardware optimized to large data
  - Algorithms covered by patents
  - Algorithms subject to export controls (from USA)

Using One Way Hash

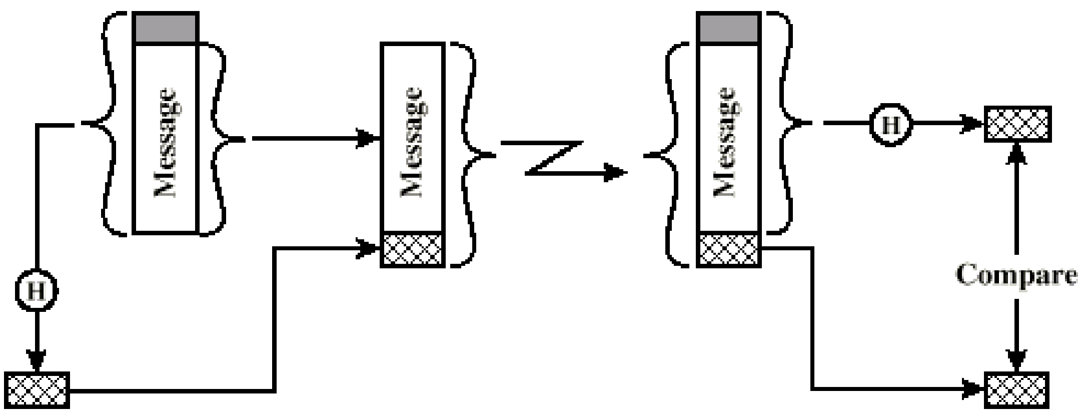


(a) Using conventional encryption

only sender and receiver share encryption key



(b) Using public-key encryption

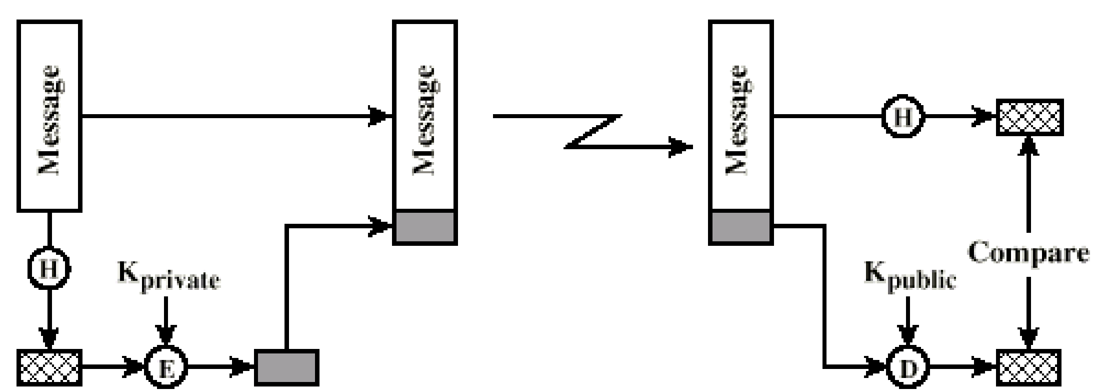


(c) Using secret value

no encryption for message authentication both parties share a common secret value

Bob

-wants to send a digitally signed message to Alice



Secure Hash Functions

- Hash function must have following properties:
  - Can be applied to any size data block
  - Produce fixed length output
  - Easy to compute
  - Not feasible to reverse
  - Not feasible to find two message that give the same hash

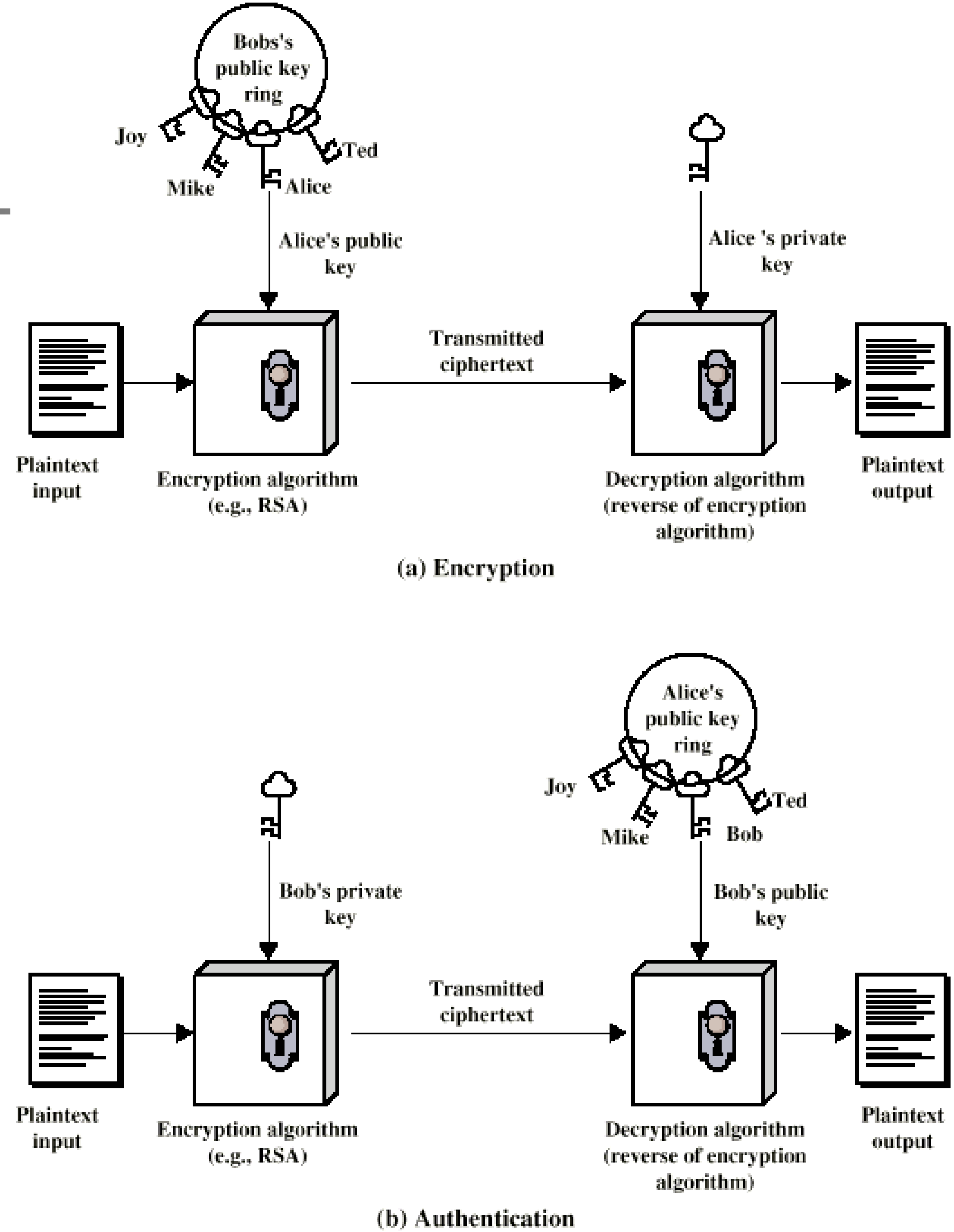
SHA-1

- Secure Hash Algorithm 1
- Input message less than 2^{64} bits
  - Processed in 512 bit blocks
- Output 160 bit digest

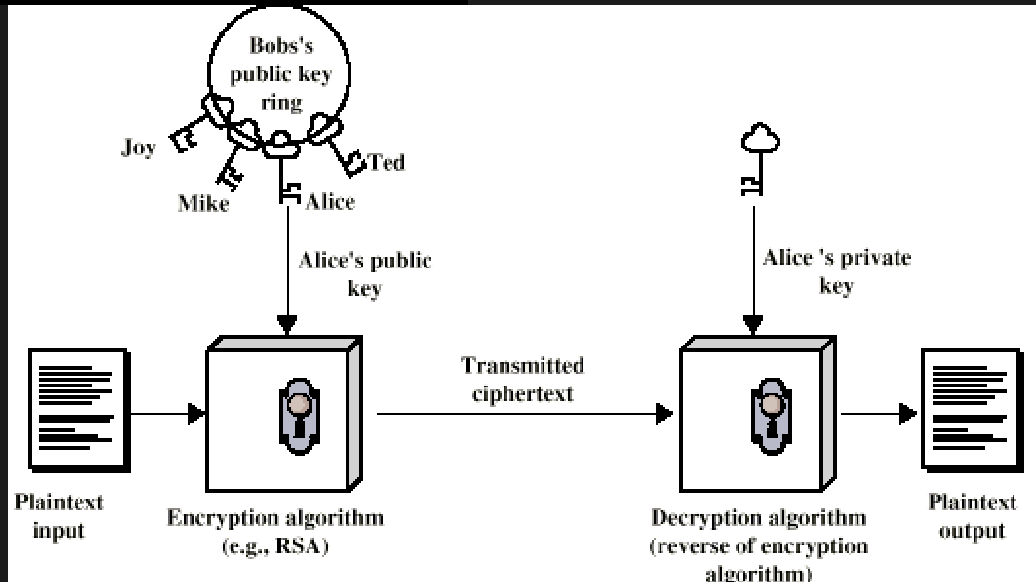
Public Key Encryption

- Based on mathematical algorithms
- Asymmetric
  - Use two separate keys
- Ingredients
  - Plain text
  - Encryption algorithm
  - Public and private key
  - Cipher text
  - Decryption algorithm

Public Key Encryption (diag)



Bob



(a) Encryption

Public Key Encryption - Operation

- One key made public
  - Used for encryption
- Other kept private
  - Used for decryption
- Infeasible to determine decryption key given encryption key and algorithm
- Either key can be used for encryption, the other for decryption

Steps

- User generates pair of keys
- User places one key in public domain
- To send a message to user, encrypt using public key
- User decrypts using private key

Digital Signature

- Sender encrypts message with their private key
- Receiver can decrypt using senders public key
- This authenticates sender, who is only person who has the matching key
- Does not give privacy of data
  - Decrypt key is public

RSA Algorithm

Key Generation

Select p, q	p and q both prime
Calculate $n = p \times q$	
Calculate $\phi(n) = (p-1)(q-1)$	
Select integer e	$\gcd(\phi(n), e) = 1;\ 1 < e < \phi(n)$
Calculate d	$d = e^{-1} \bmod \phi(n)$
Public key	$KU = \{e, n\}$
Private key	$KR = \{d, n\}$

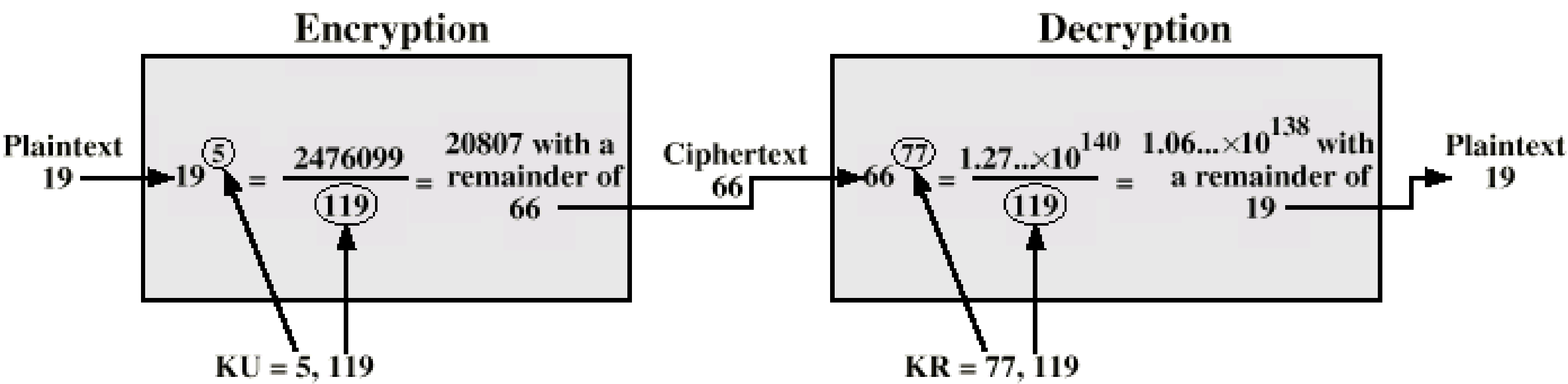
Encryption

Plaintext:	$M < n$
Ciphertext:	$C = M^e \pmod{n}$

Decryption

Ciphertext:	C
Plaintext:	$M = C^d \pmod{n}$

RSA Example



Encryption
Decryption
Plaintext
19
19
5
=
2476099
119
=
20807 with a
remainder of
66
Ciphertext
66
66
77
=
1.27...×10140
119
=
1.06...×10138 with
a remainder of
19
Plaintext
19
KU = 5, 119
KR = 77, 119