Aalto University
School of Electrical
Engineering

Basic Principles in Networking

Principles of Cryptography

Stephan Sigg

Department of Communications and Networking
Aalto University, School of Electrical Engineering
stephan.sigg@aalto.fi

Version 1.0

Aalto University
School of Electrical
Engineering

Motivation (5 min)

Cyber Security – Top 10 threats

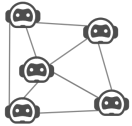
Aalto University
School of Electrical
Engineering

Part I (20 min)

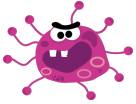
Introduction
Principles of Cryptography

Networks under attack

Networks under attack



Botnet:

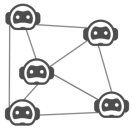


Virus:

Worm:

Trojan horse:

Networks under attack



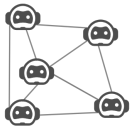
Botnet: Compromised hosts, organized in a network of thousands of similarly compromised devices. Utilized for spam e-mail distribution or distributed denial-of-service attacks

Virus:

Worm:

Trojan horse:

Networks under attack



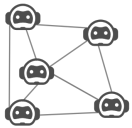
Botnet: Compromised hosts, organized in a network of thousands of similarly compromised devices. Utilized for spam e-mail distribution or distributed denial-of-service attacks

Virus: Require user interaction to infect the device. Example: Email attachment containing malicious executable code. Often self-replicating: sending malware to addresses from the addressbook of the infected device

Worm:

Trojan horse:

Networks under attack



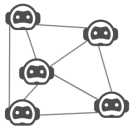
Botnet: Compromised hosts, organized in a network of thousands of similarly compromised devices. Utilized for spam e-mail distribution or distributed denial-of-service attacks

Virus: Require user interaction to infect the device. Example: Email attachment containing malicious executable code. Often self-replicating: sending malware to addresses from the addressbook of the infected device

Worm: Can enter a device without explicit user interaction. Example: Running a vulnerable network appliction to which malware can be sent. Often self-replicating: The worm scans the network for further targets

Trojan horse:

Networks under attack



Botnet: Compromised hosts, organized in a network of thousands of similarly compromised devices. Utilized for spam e-mail distribution or distributed denial-of-service attacks

Virus: Require user interaction to infect the device. Example: Email attachment containing malicious executable code. Often self-replicating: sending malware to addresses from the addressbook of the infected device

Worm: Can enter a device without explicit user interaction. Example: Running a vulnerable network appliction to which malware can be sent. Often self-replicating: The worm scans the network for further targets

Trojan horse: Hidden part of some otherwise useful software. Executed in the background, without notice

Networks under attack






Malware is pervasive and costly to defend against

Task: While following this course, think about what computer network designers can do to defend connected devices from malware







Bad guys perspective

Denial of Service attacks

DoS attacks

Renders a network, host or other piece of infrastructure unusable by legitimate users. E.g. Web servers, email servers, DNS servers and institutional networks.

Bad guys perspective

Types of DoS attacks

Vulnerability attack Sending few well-crafted messages to a vulnerable application or operating system. With the right sequence of packets, the service can stop or the host can crash

Bad guys perspective

Types of DoS attacks

Vulnerability attack Sending **well-crafted messages** to a **vulnerable** application or operating system. With the right sequence of packets, the service can stop or the host can crash

Bandwidth flooding Sending a deluge of packets to the targeted host. Due to the vast amount of packets, the target's access link becomes clogged. Legitimate packets can no longer reach the host.

Bad guys perspective

Types of DoS attacks

Vulnerability attack Sending **well-crafted messages** to a **vulnerable** application or operating system. With the right sequence of packets, the service can stop or the host can crash

Bandwidth flooding Sending a **deluge of packets** to the targeted host. Due to the vast amount of packets, the target's **access link becomes clogged**. Legitimate packets can no longer reach the host.

Connection flooding Establishing a large number of half-open or fully open TCP connections so that the host stops accepting legitimate connections due to the high load.

Bad guys perspective

Distributed Denial of Service attack

Denial of Service attack Attacker tries to send traffic at a rate that matches at least the Servers access rate R.

Bad guys perspective

Distributed Denial of Service attack

Denial of Service attack Attacker tries to send traffic at a rate that matches at least the Servers access rate R.

- If R is very large, such attack might not be feasible for a single host

Bad guys perspective

Distributed Denial of Service attack

Denial of Service attack Attacker tries to send traffic at a rate that matches at least the Servers access rate R.

- If R is very large, such attack **might not be feasible for a single host**

Distributed denial of Service attack Attacker controls multiple sources and has each source generate traffic towards the target

Bad guys perspective

Distributed Denial of Service attack

Denial of Service attack Attacker tries to send traffic at a rate that matches at least the Servers access rate R.

- If R is very large, such attack **might not be feasible for a single host**

Distributed denial of Service attack Attacker controls multiple sources and has each source generate traffic towards the target

- Much harder to detect and to defend against

Bad guys perspective

Packet sniffing

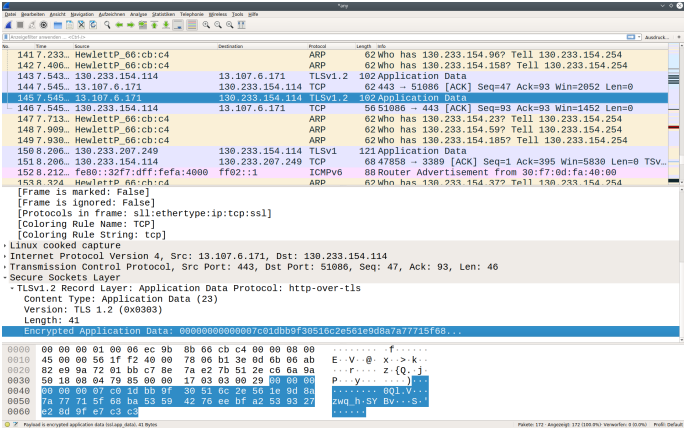
Security vulnerabilities through high number of wirelessly connected devices

Bad guys perspective

Packet sniffing

Security vulnerabilities through high number of wirelessly connected devices

- packets sent
- packet content
- private/sensitive information
- connection habits, social ties, patterns, ...



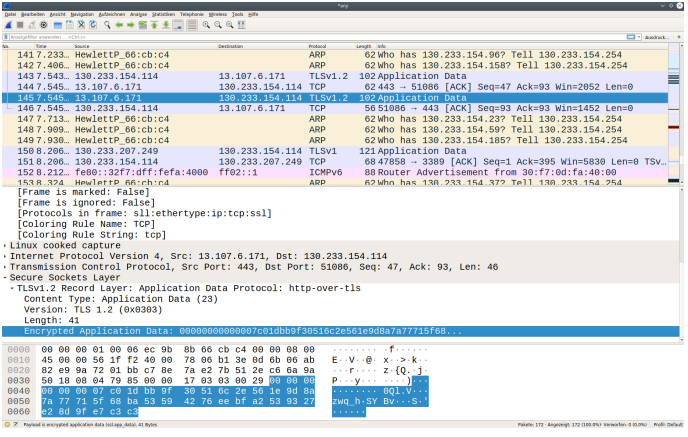
Bad guys perspective

Packet sniffing

Security vulnerabilities through high number of wirelessly connected devices

- packets sent
- packet content
- private/sensitive information
- connection habits, social ties, patterns, ...

Solution: Encryption



Bad guys perspective

Masquerading

Creating a packet with **arbitrary source address, packet content and destination address**, a receiver might be disguised of the true sender.

Bad guys perspective

Masquerading

Creating a packet with **arbitrary source address, packet content and destination address**, a receiver might be disguised of the true sender.

IP Spoofing

Injecting packets with false source address into the internet

Bad guys perspective

Masquerading

Creating a packet with **arbitrary source address, packet content and destination address**, a receiver might be disguised of the true sender.

IP Spoofing

Injecting packets with false source address into the internet

Solution: End-point authentication

Bad guys perspective

Man-in-the-middle attacks

An attacker might reside in one node within the communication path

- a compromised router,
- a software module on one of the end-hosts at a lower layer in the protocol stack

Bad guys perspective

Man-in-the-middle attacks

An attacker might reside in one node within the communication path

- a compromised router,
- a software module on one of the end-hosts at a lower layer in the protocol stack

MitM capabilities

Sniffing packets; inject, modify or delete packets

Bad guys perspective

Man-in-the-middle attacks

An attacker might reside in one node within the communication path

- a compromised router,
- a software module on one of the end-hosts at a lower layer in the protocol stack

MitM capabilities

Sniffing packets; inject, modify or delete packets

Solution: Establish data integrity

Why is the internet such an insecure place?

Bruce Schneider

Why is the internet such an insecure place?

Historical perspectives

Why is the internet such an insecure place?

Historical perspectives

1961-1972: Development of packet switching Telephone network being the dominant communication network, first computer connections were cirquit switched; packet-switching over multiple hops just evolving

Why is the internet such an insecure place?

Historical perspectives

1961-1972: Development of packet switching Telephone network being the dominant communication network, first computer connections were cirquit switched; packet-switching over multiple hops just evolving

1972-1980: Proprietary networks and internetworking Large stand alone networks (ARPAnet, ALOHANet, telenet, Cyclades, ...) were connected and TCP/UDP/IP were developed.

Why is the internet such an insecure place?

Historical perspectives

1961-1972: Development of packet switching Telephone network being the dominant communication network, first computer connections were cirquit switched; packet-switching over multiple hops just evolving

1972-1980: Proprietary networks and internetworking Large stand alone networks (ARPAnet, ALOHANet, telenet, Cyclades, ...) were connected and TCP/UDP/IP were developed.

1980-1990: A proliferation of networks Continuous growth of networks and linking Universities together created the internet; Birth of DNS

Why is the internet such an insecure place?

Historical perspectives

1961-1972: Development of packet switching Telephone network being the dominant communication network, first computer connections were cirquit switched; packet-switching over multiple hops just evolving

1972-1980: Proprietary networks and internetworking Large stand alone networks (ARPAnet, ALOHANet, telenet, Cyclades, ...) were connected and TCP/UDP/IP were developed.

1980-1990: A proliferation of networks Continuous growth of networks and linking Universities together created the internet; Birth of DNS

1990-2000: The internet explosion Invention of the World-wide-web by Tim Berners-Lee at CERN

Why is the internet such an insecure place?

Historical perspectives

1961-1972: Development of packet switching Telephone network being the dominant communication network, first computer connections were cirquit switched; packet-switching over multiple hops just evolving

1972-1980: Proprietary networks and internetworking Large stand alone networks (ARPAnet, ALOHANet, telenet, Cyclades, ...) were connected and TCP/UDP/IP were developed.

1980-1990: A proliferation of networks Continuous growth of networks and linking Universities together created the internet; Birth of DNS

1990-2000: The internet explosion Invention of the World-wide-web by Tim Berners-Lee at CERN

2000-today New applications, content distribution, internet telephony, wireless access, security, P2P networking

Desirable properties of secure communication

Principles of Cryptography

Desirable properties of secure communication

Confidentiality

Message integrity

End-point Authentication

Operational security

Principles of Cryptography

Desirable properties of secure communication

Confidentiality	Only the sender and receiver should be able to understand the contents of a message
Message integrity	
End-point Authentication	
Operational security	

Principles of Cryptography

Desirable properties of secure communication

Confidentiality	Only the sender and receiver should be able to understand the contents of a message	Encryption
Message integrity		
End-point Authentication		
Operational security		

Principles of Cryptography

Desirable properties of secure communication

Confidentiality	Only the sender and receiver should be able to understand the contents of a message	Encryption
Message integrity	Content of the communication is not altered	
End-point Authentication		
Operational security		

Principles of Cryptography

Desirable properties of secure communication

Confidentiality	Only the sender and receiver should be able to understand the contents of a message	Encryption
Message integrity	Content of the communication is not altered	Checksumming
End-point Authentication		
Operational security		

Principles of Cryptography

Desirable properties of secure communication

Confidentiality	Only the sender and receiver should be able to understand the contents of a message	Encryption
Message integrity	Content of the communication is not altered	Checksumming
End-point Authentication	Sender and receiver should be able to confirm the identity of the other party	
Operational security		

Principles of Cryptography

Desirable properties of secure communication

Confidentiality	Only the sender and receiver should be able to understand the contents of a message	Encryption
Message integrity	Content of the communication is not altered	Checksumming
End-point Authentication	Sender and receiver should be able to confirm the identity of the other party	Authentication
Operational security		

Principles of Cryptography

Desirable properties of secure communication

Confidentiality	Only the sender and receiver should be able to understand the contents of a message	Encryption
Message integrity	Content of the communication is not altered	Checksumming
End-point Authentication	Sender and receiver should be able to confirm the identity of the other party	Authentication
Operational security	Firewalls and Intrusion Detection Systems	

Principles of Cryptography

Desirable properties of secure communication

Confidentiality	Only the sender and receiver should be able to understand the contents of a message	Encryption
Message integrity	Content of the communication is not altered	Checksumming
End-point Authentication	Sender and receiver should be able to confirm the identity of the other party	Authentication
Operational security	Firewalls and Intrusion Detection Systems	firewalls, packet inspection

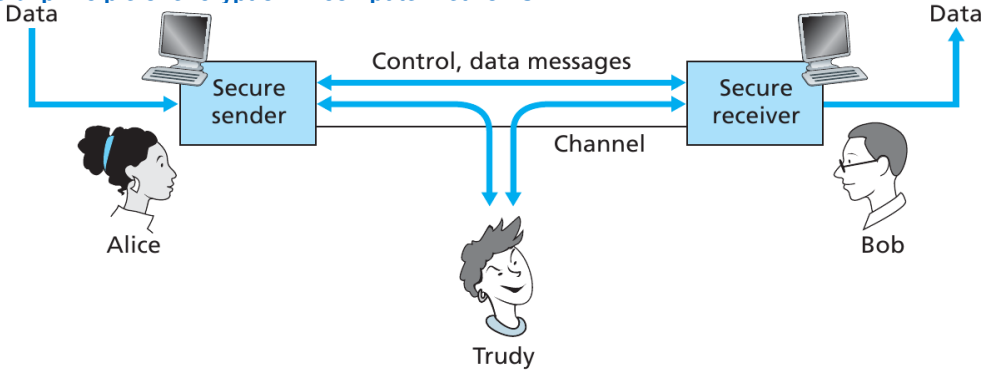
Aalto University
School of Electrical
Engineering

Part II (20 min)

Symmetric Key Cryptography
Block ciphers

Symmetric key cryptography

General principle of encryption in computer networks

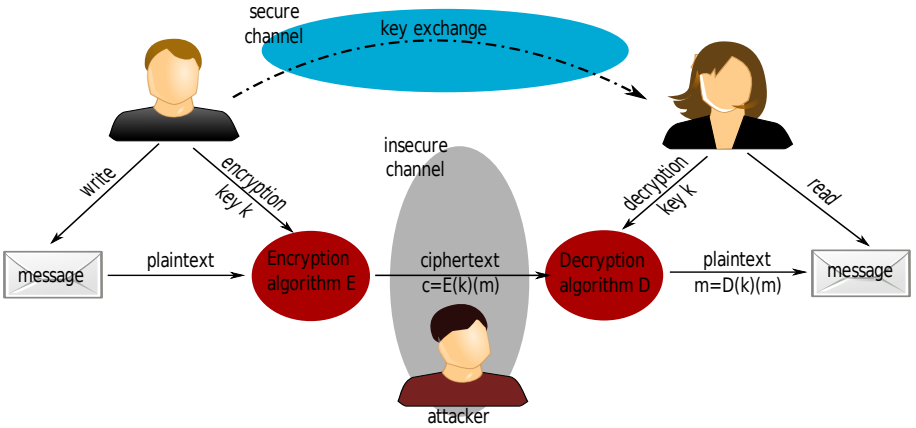


- Encryption technique known, published and standardized

Source: Computer Networking - A top-down approach; Kurose, Ross. Adisson Wesley 2012.

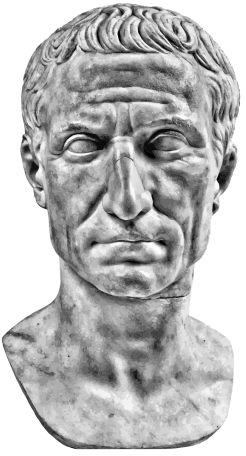
Symmetric key cryptography

Symmetric Encryption



Symmetric key cryptography

Historical encryption algorithms: Caesar Cipher



Symmetric key cryptography

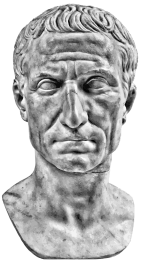
Historical encryption algorithms: Caesar Cipher

Algorithm: Cyclic shift of letters in the alphabet by k letters

Key: k

Caesar cipher with $k = 3$

Plaintext	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	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



Symmetric key cryptography

Historical encryption algorithms: Caesar Cipher

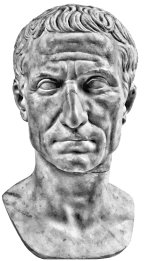
Algorithm: Cyclic shift of letters in the alphabet by k letters

Key: k

Caesar cipher with $k = 3$

Plaintext	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	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

Example ere, l oryh brx. dolfh



Symmetric key cryptography

Historical encryption algorithms: Caesar Cipher

Algorithm: Cyclic shift of letters in the alphabet by k letters

Key: k

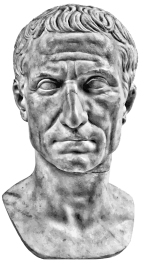
Caesar cipher with $k = 3$

Plaintext	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	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

Example

ere, l oryh brx. dolfh

bob, i love you. alice



Symmetric key cryptography

Historical encryption algorithms: Caesar Cipher

Algorithm: Cyclic shift of letters in the alphabet by k letters

Key: k

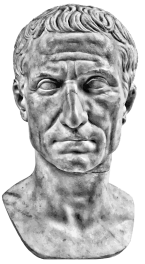
Caesar cipher with $k = 3$

Plaintext	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	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

Example: ere, l oryh brx. dolfh

bob, i love you. alice

Possible Key values



Symmetric key cryptography

Historical encryption algorithms: Caesar Cipher

Algorithm: Cyclic shift of letters in the alphabet by k letters

Key: k

Caesar cipher with $k = 3$

Plaintext	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	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

Example: ere, l oryh brx. dolfh
bob, i love you. alice

Possible Key values: 25 *(easy to brute-force if algorithm known)*

Symmetric key cryptography

Historical encryption algorithms: Monoalphabetic Cipher

Algorithm: Permutation π of the alphabet

Key: π

Monoalphabetic Cipher

Plaintext	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	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

Symmetric key cryptography

Historical encryption algorithms: Monoalphabetic Cipher

Algorithm: Permutation π of the alphabet

Key: π

Monoalphabetic Cipher

Plaintext	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	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

Example nkn, s gktc wky. mgsbc

bob, i love you. alice

Symmetric key cryptography

Historical encryption algorithms: Monoalphabetic Cipher

Algorithm: Permutation π of the alphabet

Key: π

Monoalphabetic Cipher

Plaintext	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	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

nkn, s gktc wky. mgsbc

bob, i love you. alice

Symmetric key cryptography

Historical encryption algorithms: Monoalphabetic Cipher

Algorithm: Permutation π of the alphabet

Key: π

Monoalphabetic Cipher

Plaintext	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	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

nkn, s gktc wky. mgsbc

bob, i love you. alice

Possible Key values

Symmetric key cryptography

Historical encryption algorithms: Monoalphabetic Cipher

Algorithm: Permutation π of the alphabet

Key: π

Monoalphabetic Cipher

Plaintext	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	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

nkn, s gktc wky. mgsbc

bob, i love you. alice

Possible Key values 26! (approx. 10^{26}) *(still vulnerable to statistical analysis)*

Symmetric key cryptography

Historical encryption algorithms: Polyalphabetic encryption

Algorithm: Concatenation of simple encryption schemes $C_1, \ldots, C_n$

Key: $\{C_j | j \in \{1, \ldots, n\}\}^m$

Polyalphabetic (here: Concatenation of Caesar-) ciphers: C_1, C_2, C_2, C_1, C_2

Plaintext	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
$C_1(k=5)$	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
$C_2(k=19)$	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

Symmetric key cryptography

Historical encryption algorithms: Polyalphabetic encryption

Algorithm: Concatenation of simple encryption schemes $C_1, \ldots, C_n$

Key: $\{C_j | j \in \{1, \ldots, n\}\}^m$

Polyalphabetic (here: Concatenation of Caesar-) ciphers: C_1, C_2, C_2, C_1, C_2

Plaintext	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
$C_1(k=5)$	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
$C_2(k=19)$	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 bob, i love you. alice

Symmetric key cryptography

Historical encryption algorithms: Polyalphabetic encryption

Algorithm: Concatenation of simple encryption schemes $C_1, \ldots, C_n$

Key: $\{C_j | j \in \{1, \ldots, n\}\}^m$

Polyalphabetic (here: Concatenation of Caesar-) ciphers: C_1, C_2, C_2, C_1, C_2

Plaintext	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
$C_1(k=5)$	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
$C_2(k=19)$	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

bob, i love you. alice

ghu, n etox dhz. tenvj

Symmetric key cryptography

Historical encryption algorithms: Polyalphabetic encryption

Algorithm: Concatenation of simple encryption schemes $C_1, \ldots, C_n$

Key: $\{C_j | j \in \{1, \ldots, n\}\}^m$

Polyalphabetic (here: Concatenation of Caesar-) ciphers: C_1, C_2, C_2, C_1, C_2

Plaintext	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
$C_1(k=5)$	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
$C_2(k=19)$	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 bob, i love you. alice

ghu, n etox dhz. tenvj

Possible Key values

Symmetric key cryptography

Historical encryption algorithms: Polyalphabetic encryption

Algorithm: Concatenation of simple encryption schemes $C_1, \ldots, C_n$

Key: $\{C_j | j \in \{1, \ldots, n\}\}^m$

Polyalphabetic (here: Concatenation of Caesar-) ciphers: C_1, C_2, C_2, C_1, C_2

Plaintext	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
$C_1(k=5)$	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
$C_2(k=19)$	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 bob, i love you. alice

ghu, n etox dhz. tenvj

Possible Key values 25^m

Symmetric key cryptography

Cryptographic attacks

Symmetric key cryptography

Cryptographic attacks

Ciphertext-only Intruder has access only to the ciphertext with no certain information about the contents of the plaintext message (e.g. statistical analysis).

Symmetric key cryptography

Cryptographic attacks

Ciphertext-only Intruder has access only to the ciphertext with no certain information about the contents of the plaintext message (e.g. statistical analysis).

Known-plaintext Intruder knows some of the plaintext that is to be found in the ciphertext (e.g. names, protocol headers, ...)

Symmetric key cryptography

Cryptographic attacks

Ciphertext-only Intruder has access only to the ciphertext with no certain information about the contents of the plaintext message (e.g. statistical analysis).

Known-plaintext Intruder knows some of the plaintext that is to be found in the ciphertext (e.g. names, protocol headers, ...)

Chosen-plaintext Intruder is able to choose the plaintext message and obtain its corresponding ciphertext (The quick brown fox jumps over the lazy dog)

Block Ciphers

Block ciphers are employed, for instance, in PGP (secure e-mail), SSl (securing TCP connections), IPsec (securing network-layer transport)

Block Ciphers

Block ciphers are employed, for instance, in PGP (secure e-mail), SSl (securing TCP connections), IPsec (securing network-layer transport)

Concept of block ciphers

- Message for encryption processed in blocks of k bits
- One-to-one mapping for each block

Block Ciphers

Block ciphers are employed, for instance, in PGP (secure e-mail), SSl (securing TCP connections), IPsec (securing network-layer transport)

Concept of block ciphers

- Message for encryption processed in blocks of k bits
- One-to-one mapping for each block

Example: ($k = 3$)

input	000	001	010	011	100	101	110	111
output	110	111	101	100	011	010	000	001

Block Ciphers

Block ciphers are employed, for instance, in PGP (secure e-mail), SSl (securing TCP connections), IPsec (securing network-layer transport)

Concept of block ciphers

- Message for encryption processed in blocks of k bits
- One-to-one mapping for each block

Possible Key values

Example: ($k = 3$)

input	000	001	010	011	100	101	110	111
output	110	111	101	100	011	010	000	001

Block Ciphers

Block ciphers are employed, for instance, in PGP (secure e-mail), SSl (securing TCP connections), IPsec (securing network-layer transport)

Concept of block ciphers

- Message for encryption processed in blocks of k bits
- One-to-one mapping for each block

Possible Key values

$2^3! = 40320$

Example: ($k = 3$)

input	000	001	010	011	100	101	110	111
output	110	111	101	100	011	010	000	001

Block Ciphers

Block ciphers are employed, for instance, in PGP (secure e-mail), SSl (securing TCP connections), IPsec (securing network-layer transport)

Concept of block ciphers

- Message for encryption processed in blocks of k bits
- One-to-one mapping for each block

Possible Key values

$2^3! = 40320$

Example: ($k = 3$)

input	000	001	010	011	100	101	110	111
output	110	111	101	100	011	010	000	001

input	0	1	0	1	1	0	0	0	1	1	1	1
output												

Block Ciphers

Block ciphers are employed, for instance, in PGP (secure e-mail), SSl (securing TCP connections), IPsec (securing network-layer transport)

Concept of block ciphers

- Message for encryption processed in blocks of k bits
- One-to-one mapping for each block

Possible Key values

$2^3! = 40320$

Example: ($k = 3$)

input	000	001	010	011	100	101	110	111
output	110	111	101	100	011	010	000	001

input	0	1	0	1	1	0	0	0	1	1	1	1
output	1	0	1	0	0	0	1	1	1	0	0	1

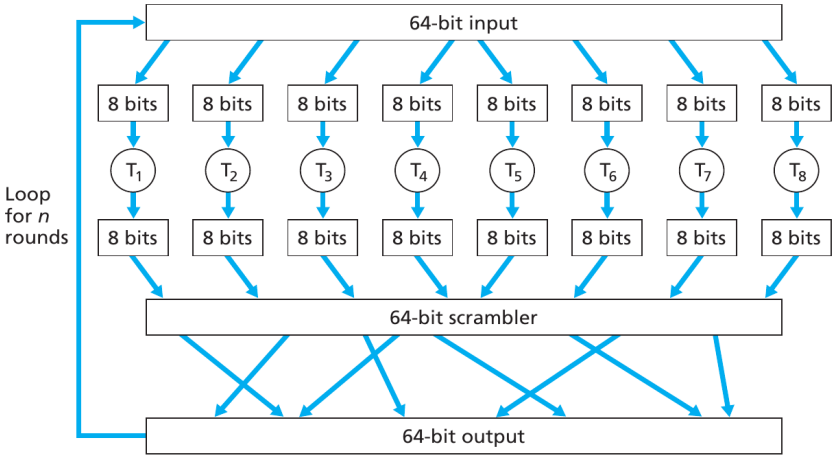
Block Ciphers

Example for a full block cipher

Using 64 bit input *(2^{64} different mappings)*

Encryption includes *n* cycles

Popular block ciphers today: e.g. DES, 3DES, AES



Source: Computer Networking - A top-down approach; Kurose, Ross. Adisson Wesley 2012.

Cipher block chaining

Problem with plain block ciphers: Repetition of text fragments might disclose information on the cipher. For instance: “HTTP/1.1”

How to resolve this problem?

Cipher block chaining

Problem with plain block ciphers:
Repetition of text fragments might disclose information on the cipher.
For instance: “HTTP/1.1”

Solution Change the cipher in each round by adding randomness

Cipher block chaining

Problem with plain block ciphers:
Repetition of text fragments might disclose information on the cipher.
For instance: “HTTP/1.1”

Solution Change the cipher in each round by adding randomness

Procedure for ciphertext chaining:

1. Random Initialization Vector $c(0)$ shared with receiver in cleartext

Cipher block chaining

Problem with plain block ciphers:
Repetition of text fragments might disclose information on the cipher.
For instance: “HTTP/1.1”

Solution Change the cipher in each round by adding randomness

Procedure for ciphertext chaining:

1. Random Initialization Vector $c(0)$ shared with receiver in cleartext
2. Ciphertext for the first block: $c(1) = K_S(m(1) \oplus c(0))$

Cipher block chaining

Problem with plain block ciphers:
Repetition of text fragments might disclose information on the cipher.
For instance: “HTTP/1.1”

Solution Change the cipher in each round by adding randomness

Procedure for ciphertext chaining:

1. Random Initialization Vector $c(0)$ shared with receiver in cleartext
2. Ciphertext for the first block: $c(1) = K_S(m(1) \oplus c(0))$
3. Ciphertext for the i-th block: $c(i) = K_S(m(i) \oplus c(i-1))$

Cipher block chaining – example

Example:

input	000	001	010	011	100	101	110	111
output	110	111	101	100	011	010	000	001

input	0	1	0	0	1	0	0	1	0
$c(0)$	0	0	1						
output									

Cipher block chaining – example

Example:

input	000	001	010	011	100	101	110	111
output	110	111	101	100	011	010	000	001

input	0	1	0	0	1	0	0	1	0
$c(0)$	0	0	1						
$m(1) \oplus c(0)$	0	1	1						
output									

Cipher block chaining – example

Example:

input	000	001	010	011	100	101	110	111
output	110	111	101	100	011	010	000	001

input	0	1	0	0	1	0	0	1	0
$c(0)$	0	0	1						
$m(1) \oplus c(0)$	0	1	1						
output	1	0	0						

Cipher block chaining – example

Example:

input	000	001	010	011	100	101	110	111
output	110	111	101	100	011	010	000	001

input	0	1	0	0	1	0	0	1	0
$c(0)$	0	0	1						
$m(1) \oplus c(0)$	0	1	1						
$c(1)$				1	0	0			
$m(2) \oplus c(1)$				1	1	0			
output	1	0	0						

Cipher block chaining – example

Example:

input	000	001	010	011	100	101	110	111
output	110	111	101	100	011	010	000	001

input	0	1	0	0	1	0	0	1	0
$c(0)$	0	0	1						
$m(1) \oplus c(0)$	0	1	1						
$c(1)$				1	0	0			
$m(2) \oplus c(1)$				1	1	0			
output	1	0	0	0	0	0			

Cipher block chaining – example

Example:

input	000	001	010	011	100	101	110	111
output	110	111	101	100	011	010	000	001

input	0	1	0	0	1	0	0	1	0
$c(0)$	0	0	1						
$m(1) \oplus c(0)$	0	1	1						
$c(1)$				1	0	0			
$m(2) \oplus c(1)$				1	1	0			
$c(2)$							0	0	0
$m(3) \oplus c(1)$							0	1	0
output	1	0	0	0	0	0			

Cipher block chaining – example

Example:

input	000	001	010	011	100	101	110	111
output	110	111	101	100	011	010	000	001

input	0	1	0	0	1	0	0	1	0
$c(0)$	0	0	1						
$m(1) \oplus c(0)$	0	1	1						
$c(1)$				1	0	0			
$m(2) \oplus c(1)$				1	1	0			
$c(2)$							0	0	0
$m(3) \oplus c(1)$							0	1	0
output	1	0	0	0	0	0	1	0	1

Aalto University
School of Electrical
Engineering

Video (5 min)

They are working for us

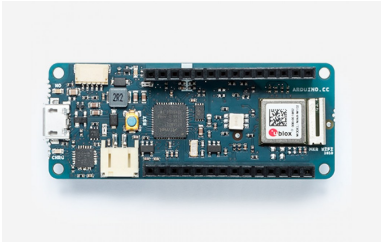
Aalto University
School of Electrical
Engineering

Exercise briefing (15 min)

Cryptography

Exercise briefing

- Additional pracical guidance
- Setting you up for the exercises
- Q&A



Questions?

Stephan Sigg
stephan.sigg@aalto.fi

Arun Katuwal
arun.katuwal@aalto.fi

Dheeraj Chandrashekar
dheeraj.chandrashekar@aalto.fi

Literature

- J.F. Kurose,K.W. Ross: Computer Networking: A Top-Down approach (7th edition), Pearson, 2016.
- J.F. Kurose,K.W. Ross: Computer Networking: A Top-Down approach (6th edition), Addison-Wesley, 2012.