Computer Networks

-Network management and security-

College of Information Science and Engineering
Ritsumeikan University

RITSUMEIKAN UNIVERSITY

W13 short test (1)

- The data link layer can be split into two sublayers, the Medium Access Control (MAC) and the logical link control sublayer.
- In mobile phone systems, a geographic region is divided up into cells. In the center of these, there are base stations where all the telephones in there transmit.
- Broadcasting an Access Points SSID is optional. - True
- With wireless, stations do not have to authenticate before sending frames via Access Points. - False
- In the context of mobile networks, what is handoff?
    - Handoff is about transferring the ownership: when a mobile phone physically leaves a cell, the base station asks the surrounding base station how much signal they are getting from it, then the phone switches channels.

W13 short test (2)

- In cellular networks, what are the basic type of channels, and what is their job?
  - Base to mobile, managing the system: control channels. Base to mobile, alert users to calls: paging channels. Bidirectional for call setup and channel assignment: access channels. Bidirectional for carrying voice, fax, data: data channels.
- What are the two modes to connect with 802.11, and how do they work?
  - Infrastructure mode: connect clients (e.g., laptops, smartphones, etc.) to another network (e.g., company intranet or the Internet), where the client sends and receives its packets via an Access Point. Ad hoc mode: A collection of computers that are associated so that they can send directly frames to each other, without using Access Points.

W13 short test (3)

- What is the purpose of the Network Allocation Vector?
  - It is used in virtual sensing, where each station keeps a logical record of when the channel is in use using the NAV. Each frame carries this NAV field showing how long the sequence (of which this frame is part of) will take to complete. Stations that overhear this will know that the channel will be busy for the period indicated by the NAV.

W13 recap (1)

- Real-time audio and video must be played out at some predetermined rate to be useful (different from normal Web traffic)
- There is enough bandwidth, but the key issue for streaming applications is network delay
- Digital audio is the digital representation of an audio wave that can be used to recreate it: ADC
- Taking digital values to produce an analog electrical voltage: DAC
- Audio is usually compressed to reduce bandwidth needs and transfer times (lossy vs lossless encoding and decoding)
- Audio compression can be done in two ways: waveform coding and perceptual coding
- Worldwide standard for video compression comes from the MPEG, using the JPEG algorithm and three different kind of frames (I, P, B)

W13 recap (2)

- VoD: streaming a video that is already stored on a server
- A media player designed for streaming is needed: manage user interface, decrypt file, handle transmission errors, decompress content, eliminate jitter
- Dealing with errors depends on weather a TCP-based transport like HTTP is used or UDP-based like RTP
- The basic function of RTP is to multiplex several real-time data streams onto a single stream of UDP packets
- RTCP handles feedback, synchronization, and the user interface
- Streaming using DASH: the streaming server first encodes the movies at multiple resolutions and frame rates, and has them stored in many files
- Apple's HLS supported by browsers, game consoles, TVs: similar idea to DASH, with additional features

W13 recap (3)

- Live streaming using IPTV is widespread nowadays
- When streaming live events, news broadcast, etc. when the user logs onto the site covering the live event, no video is shown until the buffer fills
- Biggest difference streaming a movie and Voice over IP/Internet telephony is the need for low latency that is difficult to achieve
- Internet conferencing systems using H.323 and SIP
  - both compatible with the Internet
  - SIP has a modular architecture
  - H.323 includes a full protocol stack
  - both use RTP/RTCP and supports encryption

Agenda

- Fundamental concepts
- Attack types
- Intrusion detection and prevention
- Cryptography
- Public-keys and Digital signatures
- Summary

Security properties

- Security quickly became a huge problem with computer networks
- *Confidentiality* is about keeping information out of the hands of unauthorized users
- *Integrity* is about ensuring that the information received was really the information sent and not modified
- *Availability* deals with preventing systems and services from becoming unusable due to crashes, overload, or deliberate misconfigurations
- *Authentication* deals with determining whom you are talking to before revealing sensitive information
- *Nonrepudiation* deals with signatures

Attack principles

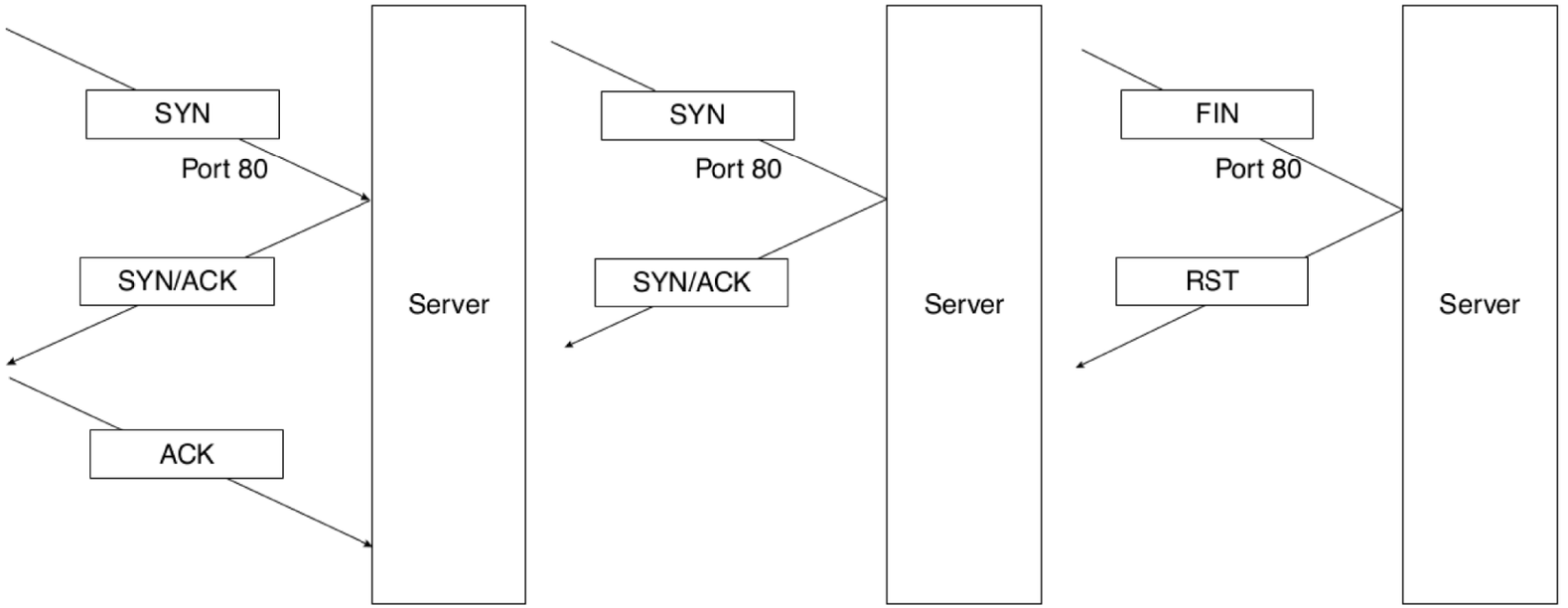
- Multiple ways to violate confidentiality, integrity, and availability
- **Reconnaissance**: the first thing for an attacker is to get to know as much about the target as possible. It is about discovering information that helps the attacker.
- **Sniffing and snooping**: an important step in many network attacks concerns the interception of network packets.
- **Spoofing**: masquerading as someone else. Spoofed network traffic pretends to originate from some other machine.
- **Disruption**: attacking the availability, for example with DoS (Denial of Service)

From threats to solutions

- Determining what to do about attackers' moves:
- Monitor the network
- Address the systems-related issues of data confidentiality
- Consider symmetric and public key cryptography
- Consider digital signatures and key management
- Look at the fundamental problem of secure authentication
- Review network technologies providing communication security
- Understand the problem of email security
- Understand social issues regarding security

Reconnaissance

- Gain information about an organization
  - social engineering, OSINT (Open Source Intelligence)
- **Port scanning**: probe a machine for active ports
  - setting up a full TCP connection is unsophisticated and logged, so *half-open scan* is used



(a) Connect scan: connection established implies port is open

(b) Half open scan: SYN/ACK reply implies port open

(c) FIN scan: RST reply implies port is closed

Sniffing, snooping

- Promiscuous mode accepts all packets on a channel
  - the attacker has a presence in the victim's network, and captures the traffic
- In a switched network, all communication is switched and attackers will not receive any of the Ethernet frames destined for the other hosts on the segment
  - attackers use MAC cloning (and switch table poisoning) to duplicate the MAC address of the host whose traffic is being sniffed (and abuse the forwarding table of self-learning Ethernet switches)
  - attackers target hosts directly using an ARP spoofing (and ARP table poisoning)
  - attackers use a MITM (Man-in-the-Middle) gateway to intercept all traffic between two hosts

Spoofing

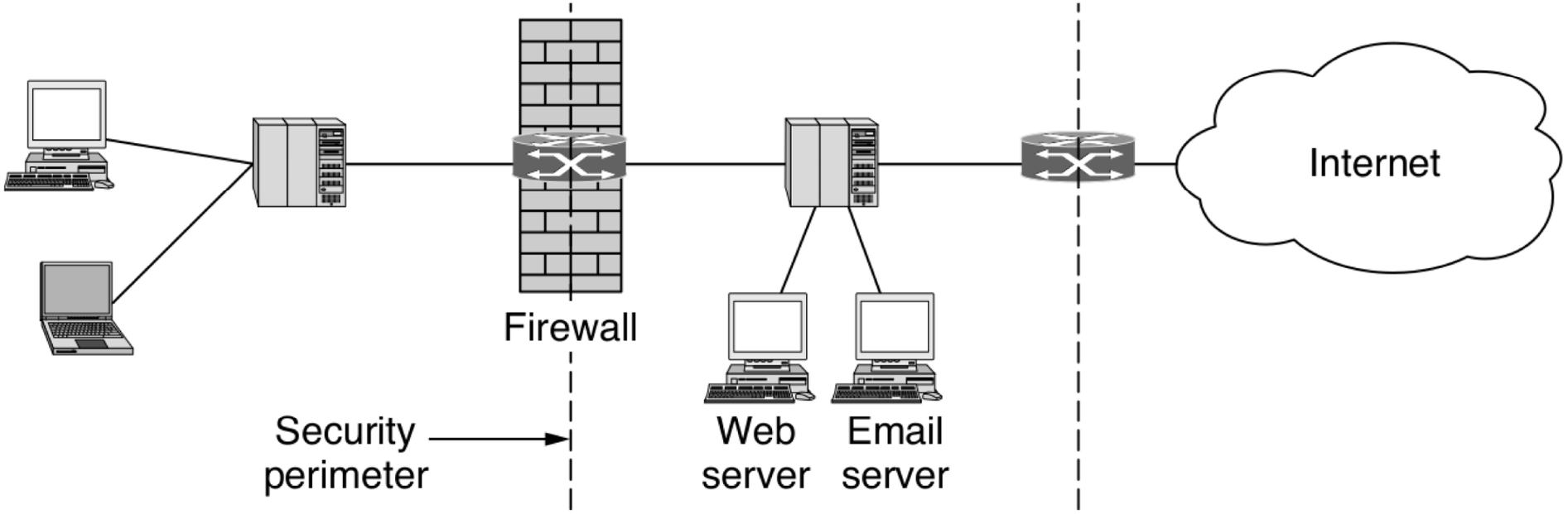
- DNS spoofing (DNS cache poisoning): redirect traffic to a fraud website that seems like the victim's intended destination by altering the DNS records
- TCP spoofing: Attackers have to find out the correct port number and sequence numbers
  - connection spoofing: the attacker sets up a new connection, pretending to be someone at a different computer
  - connection hijacking: the attacker injects data in a connection that already exists between two parties, pretending to be either of these two parties

Disruption

- Attacks on availability are known as **denial-of-service** attacks: the victim receives data it cannot handle so it becomes unresponsive
  - crashes: the attacker sends content that causes the victim to crash or hang
  - algorithmic complexity: the attacker sends data that is crafted specifically to create a lot of overhead
  - flooding/swamping: the attacker bombards the victim with a massive flood of requests or replies
- Flooding attacks became the most "popular" as those are usually easy to carry out
  - if the attack data is sent from a large number of distributed machines, it is called **DDoS** (Distributed Denial-of-Service)

Firewalls

- Danger of information leaking out, and leaking in
- A company can have many LANs connected in arbitrary ways, but all traffic to or from the company is forced through a **firewall** (no other route)
- The firewall acts as a packet filter, as it inspects each and every incoming and outgoing packet: only packets meeting some criterion described in rules formulated by the network administrator are forwarded



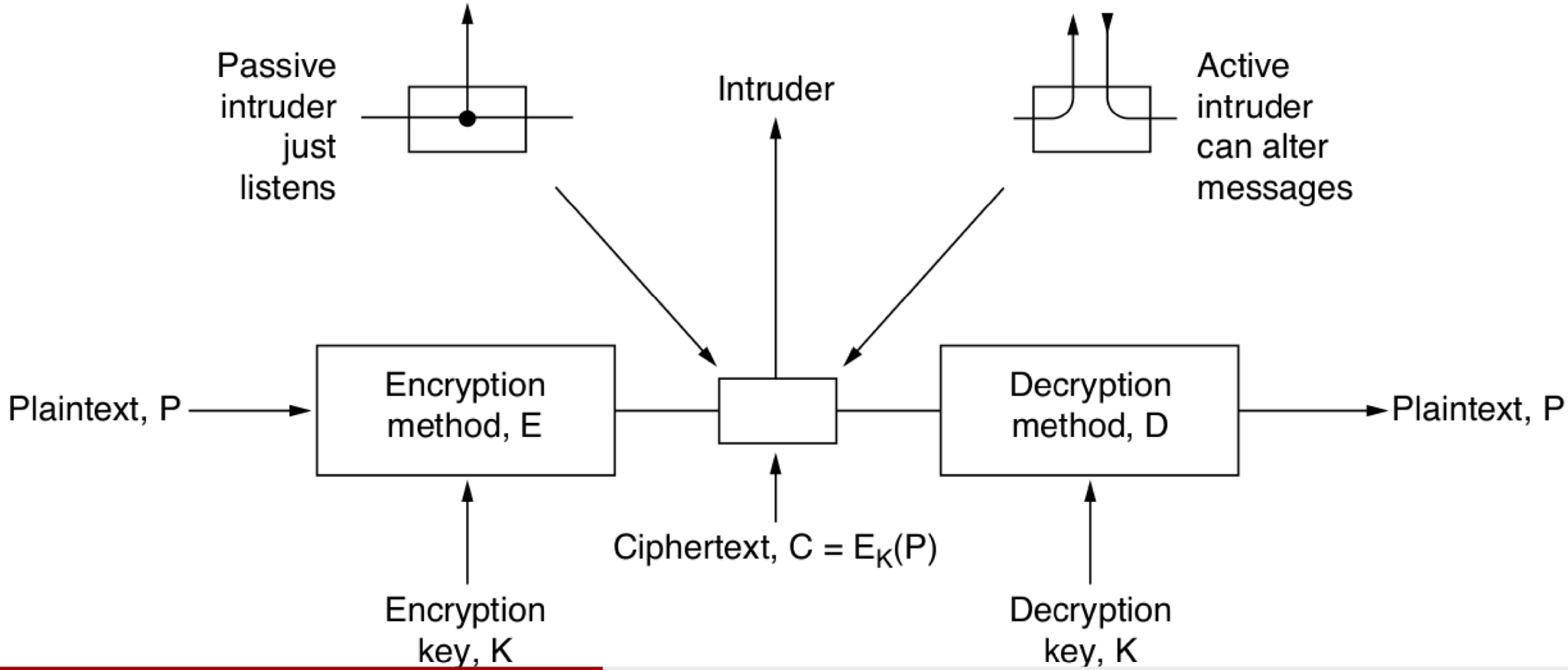
IDS

- The role of an **IDS** (Intrusion Detection System) is to detect attacks, (preferably before they can do any serious damage)
  - HIDS (Host-based IDS) works on the end-point itself (e.g., a server)
  - NIDS (Network IDS) checks the traffic for a set of machines on the network
- Signature-based IDS use patterns in terms of bytes or sequences of packets that are symptoms of already known attacks
- Anomaly-based IDS triggers on any abnormal behavior, capable of detecting new and old attacks, but without specific explanation
- IPS (Intrusion Prevention System) should detect and stop an attack
  - processing times
  - false positives vs. false negatives

Definitions

- **Cryptography** is the study of secure communications techniques
- A **cipher** is a character-for-character or bit-for-bit transformation without regard to the linguistic structure of the message, and a **code** replaces one word with another word or symbol
- Messages to be encrypted are known as the **plaintext**, transformed by a function parameterized by a **key**
- The output of the encryption process is a **ciphertext**
- **Cryptanalysis** is about breaking ciphers, and **cryptology** is about devising them

The basic encryption model



Ciphers (1)

- In a **substitution cipher**, each letter or group of letters is replaced by another letter or group of letters to disguise it

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

- **Transposition ciphers** shift the letters according to a regular system/key

M	E	G	A	B	U	C	K
7	4	5	1	2	8	3	6
p	l	e	a	s	e	t	r
a	n	s	f	e	r	o	n
e	m	i	l	l	i	o	n
d	o	l	l	a	r	s	t
o	m	y	s	w	i	s	s
b	a	n	k	a	c	c	o
u	n	t	s	i	x	t	w
o	t	w	o	a	b	c	d

Plaintext

pleasetransferonemilliondollarsto
myswissbankaccountsixtwotwo

Ciphertext

AFLLSKSOSELAWAIATOOSSCTCLNMOMANT
ESILYNTWRNNTSOWDPAEDOBUOERIRICXB

Ciphers (2)

- **One-time pad** is immune to all present and future attacks: no information in the message because all possible plaintexts of the given length are equally likely
  1. choose a random bit string as the key
  2. convert the plaintext into a bit string
  3. compute XOR of these two strings (bit-wise)

Message 1:	1001001	0100000	1101100	1101111	1110110	1100101	0100000	1111001	1101111	1110101	0101110
Pad 1:	1010010	1001011	1110010	1010101	1010010	1100011	0001011	0101010	1010111	1100110	0101011
Ciphertext:	0011011	1101011	0011110	0111010	0100100	0000110	0101011	1010011	0111000	0010011	0000101
Pad 2:	1011110	0000111	1101000	1010011	1010111	0100110	1000111	0111010	1001110	1110110	1110110
Plaintext 2:	1000101	1101100	1110110	1101001	1110011	0100000	1101100	1101001	1110110	1100101	1110011

Symmetric-key algorithms

- **Symmetric key algorithms** use the same key for encryption and decryption
- Cryptographic algorithms can be implemented in either hardware (for speed) or software (flexibility)
- **Block ciphers** take an n-bit block of plaintext as input and transform it using the key into an n-bit block of ciphertext
- **DES** (Data Encryption Standard) developed by IBM was widely adopted by the industry, but became insecure eventually as computational power increased
- **AES** (Advanced Encryption Standard) is still a widely used and very fast algorithm, supports 128, 192, and 256 bit key lengths

Public and private keys

- Distributing the keys has always been the weakest link in most cryptosystems
- The main idea behind **public-key cryptography**, where the (keyed) encryption algorithm is E, the (keyed) decryption algorithm is D, and P is the plaintext
  - $D(E(P)) = P$
  - Must be very difficult to deduce D from E
  - The encryption algorithm and its key are made public
  - The secret decryption algorithm has a private key
- **RSA** is a strong and secure public-key algorithm, requiring a 2048 bit key for good security

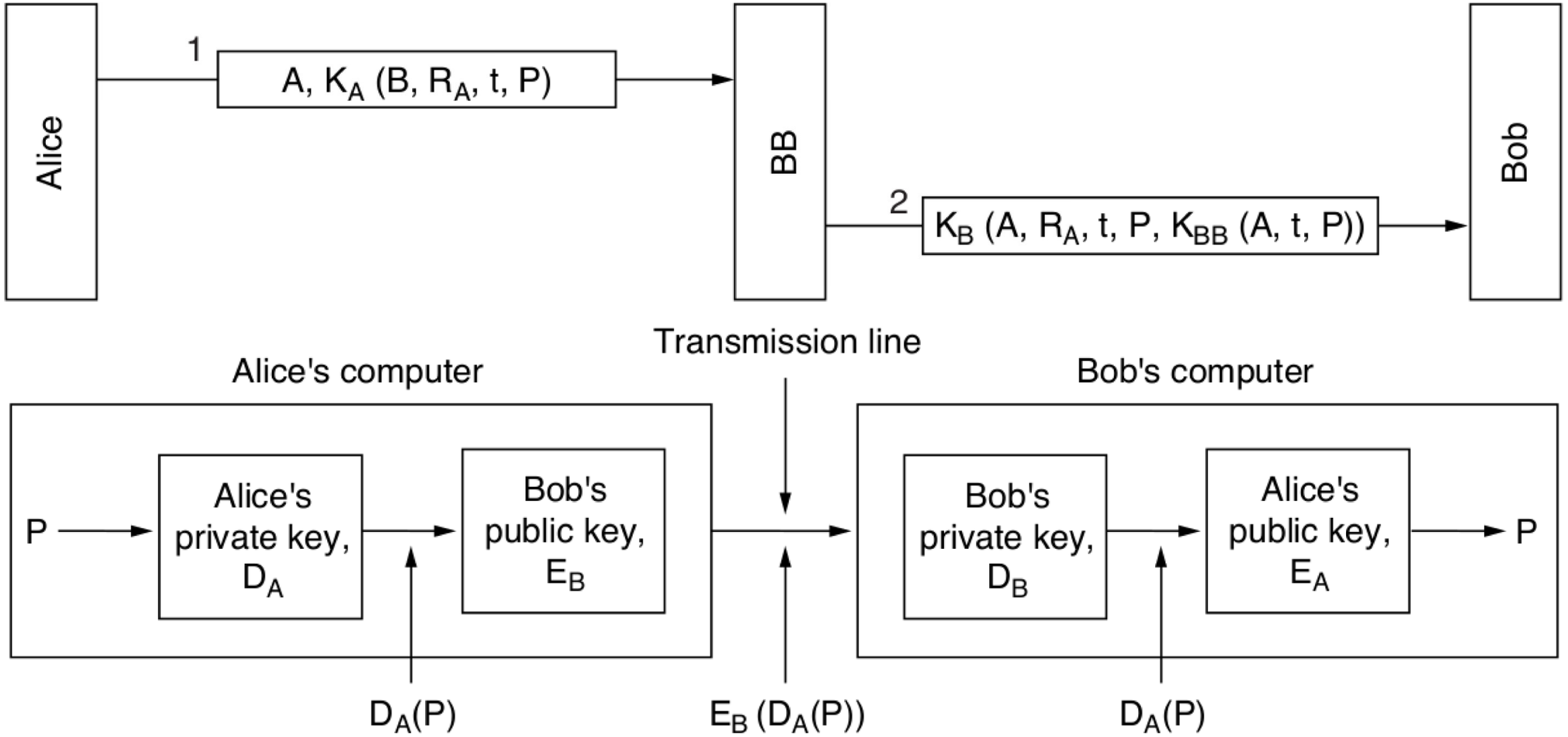
Digital signatures

- Required conditions:
  - the receiver can verify the claimed identity of the sender
  - the sender cannot later repudiate the contents of the message
  - the receiver cannot possibly have concocted the message himself

Term	Description
A	Alice (sender)
B	Bob the Banker (recipient)
P	Plaintext message Alice wants to send
BB	Big Brother (a trusted central authority)
t	Timestamp (to ensure freshness)
R_A	Random number chosen by Alice

Symmetric key	
K_A	Alice's secret key (analogous for K_B, K_{BB}, etc.)
$K_A(M)$	Message M encrypted/decrypted with Alice's secret key
Asymmetric keys	
D_A	Alice's private key (analogous for D_B, etc.)
E_A	Alice's public key (analogous for E_B, etc.)
$D_A(M)$	Message M encrypted/decrypted with Alice's private key
$E_A(M)$	Message M encrypted/decrypted with Alice's public key

Symmetric-key and Public-key signatures



W14 summary (1)

- Security properties: Confidentiality, Integrity, Availability, Authentication, Nonrepudiation
- Attack principles: Reconnaissance, Sniffing, Spoofing, Disruption
  - OSINT, port scanning
  - MAC cloning, ARP spoofing, MITM attack
  - DNS spoofing, TCP spoofing
  - denial-of-service attacks, DDoS
- The firewall acts as a packet filter, as it inspects each and every incoming and outgoing packet
- The role of an IDS is to detect attacks (signature-based or anomaly-based)
- An IPS should detect and stop an attack
- Cryptography is the study of secure communications techniques

W14 summary (2)

- Messages to be encrypted are known as the plaintext, transformed by a function parameterized by a key
- Substitution, transposition, and one-time pad ciphers
- Symmetric key algorithms
  - DES, AES
- In public-key cryptography, the encryption algorithms and its key are public, while the decryption algorithm has a private key
  - RSA
- Symmetric-key and Public-key signatures