Mobile Network Final Study

OFDM teknolojisi nedir?

In telecommunications, orthogonal frequency-division multiplexing (OFDM) is a type of digital transmission and a method of encoding digital data on multiple carrier frequencies. OFDM is a modulation format that is being used for many of the latest wireless and telecommunications standards such as The wireless LAN (WLAN) radio interfaces, The digital radio systems etc.

OFDM Avantajları, dezavantajları?

Avantajları

- High spectral efficiency as compared to other double sideband modulation schemes, spread spectrum, etc.
- Can easily adapt to severe channel conditions without complex time-domain equalization.
- Robust against narrow-band co-channel interference
- Efficient implementation using fast Fourier transform

Dezavantajları

- Sensitive to Doppler shift
- Sensitive to frequency synchronization problems
- High peak-to-average-power ratio (PAPR),

Hidden Terminal Problemini açıklayınız?

Hidden terminal problem, physical obstructions in the environment (for example, a mountain or a building) may prevent A and C from hearing each other's transmissions, even though A's and C's transmissions are indeed interfering at the destination, B.

Mobil ağlarda Indirect Routing i açıklayınız?

indirect routing: communication from correspondent to mobile goes through home agent, then forwarded to remote.

direct routing: correspondent gets foreign address of mobile, sends directly to mobile.

* An indirect routing approach is used in the mobile IP standard [RFC 5944].

switch ve router farkları?

burası komple 2021 final de çıktı!!!

3 temel Multiple access Protocol yaklaşımları(approach) nelerdir?

- **channel partitioning protocols:**
  - divide channel into smaller "pieces" (time slots, frequency or code)
  - allocate piece to node for exclusive use
  - time-division multiplexing (TDM) and frequency-division multiplexing (FDM) are used.
- **random access protocols:**
  - channel not divided, allow collisions
  - "recover" from collisions
  - More dynamic and carrier sensing
  - examples of random access MAC protocols:
    - ✓ slotted ALOHA
    - ✓ ALOHA
    - ✓ CSMA, CSMA/CD, CSMA/CA
- **taking-turns protocols:**
  - nodes take turns, but nodes with more to send can take longer turns
  - polling from central site, token passing
  - bluetooth, FDDI, token ring

CSMA yı açıklayınız?

Carrier Sense Multiple Access (CSMA) listen before transmit, if channel sensed idle: transmit entire frame , if channel sensed busy, defer transmission we can think this as don't interrupt others! But collisions can still occur.

Channel coding ve 2 temel bileşeni nedir?

- **Channel coding is necessary to minimize errors in the transmission of data**
- **Channel coding adds redundant bits to protect the source data**
- **Two categories of channel coding:**
  - Error Detection Coding
  - Error Correction Coding
- **Two types of channel codes:**
  - Block Codes (Hamming, CRC, Reed-Solomon, etc.)
  - Convolutional Codes

CSMA/CD (collision detection):
collisions detected within short time
colliding transmissions aborted,
reducing channel wastage

CSMA/CD efficiency

- T_{prop} = max prop delay between 2 nodes in LAN
- t_{trans} = time to transmit max-size frame

$$efficiency = \frac{1}{1 + 5t_{prop}/t_{trans}}$$

- efficiency goes to 1

FDMA, CDMA, TDMA nedir, açıkla?

- **Code Division Multiple Access (CDMA)** is unique "code" assigned to each user; i.e., code set partitioning
- **FDMA: frequency division multiple access:**
  - ✓ channel spectrum divided into frequency bands,
  - ✓ each station assigned fixed frequency band,
  - ✓ unused transmission time in frequency bands go idle
- **TDMA: time division multiple access:**
  - ✓ access to channel in "rounds",
  - ✓ each station gets fixed length slot (length = pkt trans time) in each round,
  - ✓ unused slots go idle

DOCSIS: data over cable service interface spec

- FDM over upstream, downstream frequency channels
- TDM upstream: some slots assigned, some have contention
  - downstream MAP frame: assigns upstream slots
  - request for upstream slots (and data) transmitted random access (binary backoff) in selected slots

CSMA - CA nedir, nasıl çalışıyor?

- CSMA/C(ollision)A(voidance) the station refrains from transmitting while counting down, even when it senses the channel to be idle.

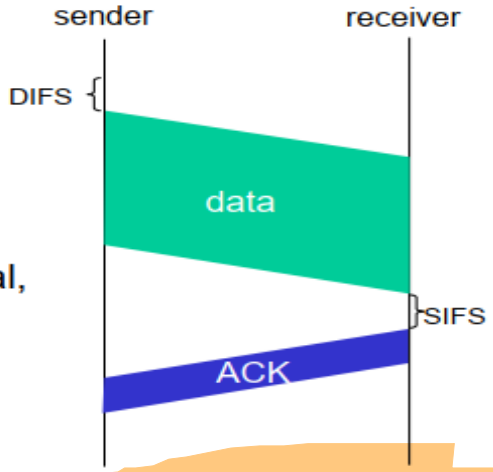
IEEE 802.11 MAC Protocol: CSMA/CA

802.11 sender

1 if sense channel idle for **DIFS** then
transmit entire frame (no CD)
2 if sense channel busy then
start random backoff time
timer counts down while channel idle
transmit when timer expires
if no ACK, increase random backoff interval, repeat 2

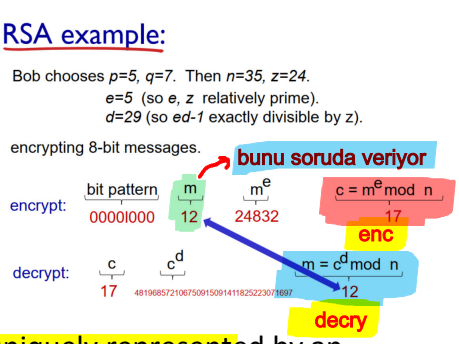
802.11 receiver

- if frame received OK
return ACK after **SIFS** (ACK needed due to hidden terminal problem)



2021 finalde Çıktı!!!!!

Recall that under Ethernet's CSMA/CD, multiple access protocol (Section 5.3.2), a station begins transmitting as soon as the channel is sensed idle. With CSMA/CA, however, the station refrains from transmitting while counting down, even when it senses the channel to be idle.



RSA Algoritmasını açıkla

RSA: Rivest, Shamir, Adelson algorithm

In RSA message is just a bit pattern because bit pattern can be uniquely represented by an integer number thus, encrypting a message is equivalent to encrypting a number.

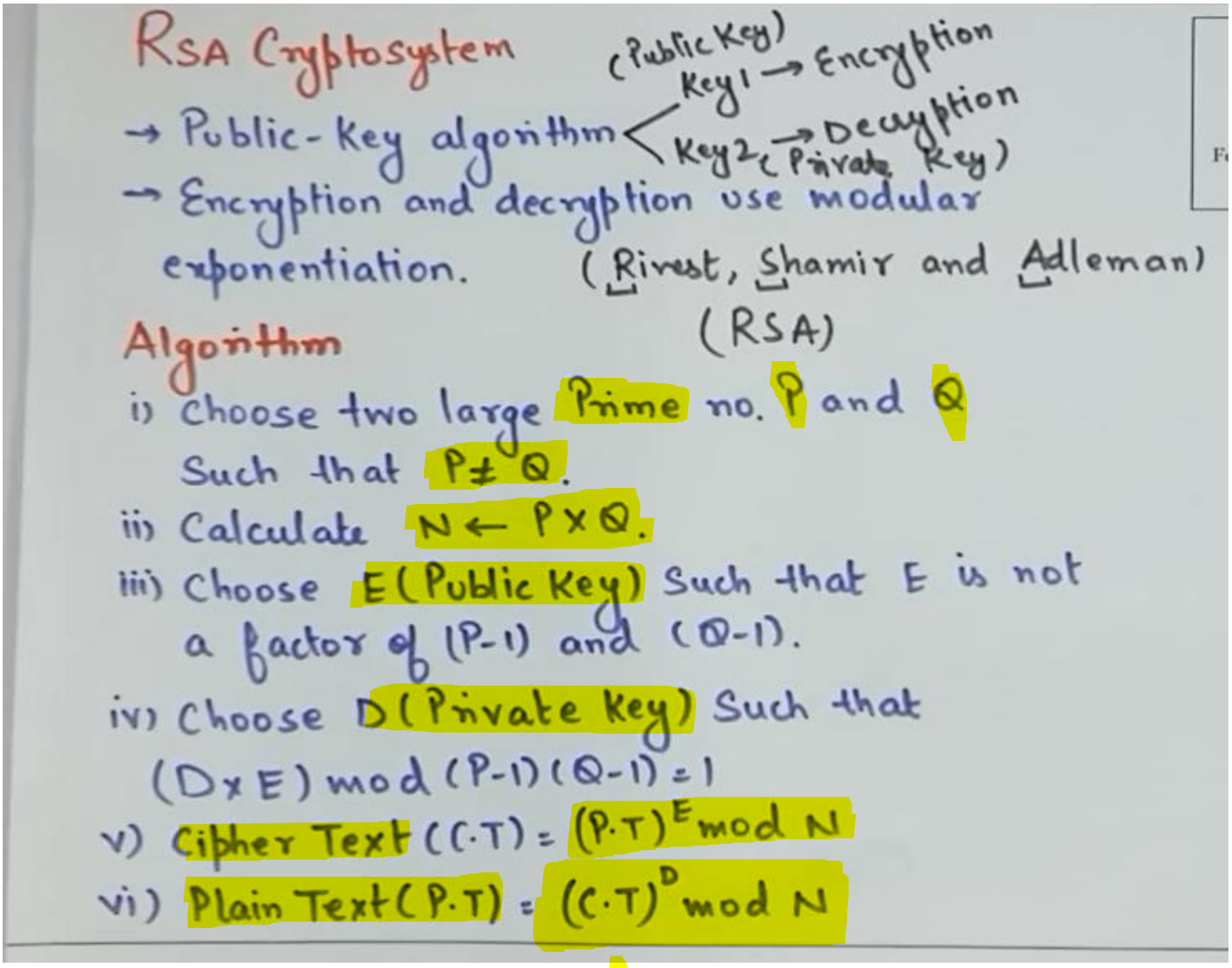
There are two interrelated components of RSA:

- The choice of the public key and the private key
- The encryption and decryption algorithm

Example:

m= 10010001 . This message is uniquely represented by the decimal number 145.

To encrypt m, we encrypt the corresponding number, which gives a new number (the ciphertext).



1. choose two large prime numbers p, q. (e.g., 1024 bits each)
2. compute $n = pq$, $z = (p-1)(q-1)$
3. choose e (with $e<n$) that has no common factors with z (e, z are "relatively prime").
4. choose d such that $ed-1$ is exactly divisible by z. (in other words: $ed \bmod z = 1$).
5. *public* key is (n,e). *private* key is (n,d).

devamı

1. to encrypt message m ($<n$), compute
$c = m^e \bmod n$

2. to decrypt received bit pattern, c, compute
$m = c^d \bmod n$

magic happens! $m = \underbrace{(m^e \bmod n)}_{c}{}^d \bmod n$

Chapter Study one by one

Chapter 9: Network Management

What are the Network management standards?

- **OSI CMIP**
  - Common Management Information Protocol
  - designed 1980's: the unifying net management standard
  - too slowly standardized
- **SNMP: Simple Network Management Protocol**
  - Internet roots (SGMP)
  - started simple
  - deployed, adopted rapidly
  - growth: size, complexity

Explain SNMP ?

SNMP overview: 4 key parts

- Management information base (MIB):
- Structure of Management Information (SMI):
- SNMP protocol
- security, administration capabilities

Components of SNMP: manager, agent, management information base(mib)

SNMP protocol: message types

- GetRequest
- GetNextRequest
- GetBulkRequest
- InformRequest
- SetRequest
- Response
- Trap

request
next
bulk
inform
set

Solving the presentation problem

1. Translate local-host format to host-independent format
2. Transmit data in host-independent format
3. Translate host-independent format to remote-host format

Potential Questions

SECTION 9.2

R4. Define the following terms: managing entity, managed device, management agent, MIB, network management protocol.

- ***Managing entity:*** control the collection, processing, analysis, display of network management information, and is used by the network manager to control the devices in the network.
- ***Managed device:*** a piece of network equipment that is under the control of the managing entity.
- ***Management agent:*** a software process running on a managed device that communicated with the managing entity and takes action on the managed device under the control of the managing entity.
- ***MIB:*** pieces of information associated with all of the managed objects in a device.
- ***Network management protocol:*** runs between the managing entity of the management agents on the managed devices, allowing the agents to alert the managing entity to potential problems, and allowing the managing entity to send commands to the management agents.

R5. What is the role of the SMI in network management?

R6. What is an important difference between a request-response message and a trap message in SNMP?

R7. What are the seven message types used in SNMP?

R8. What is meant by an "SNMP engine"?

5. The SMI is a data-definition language used to defined the pieces of information in an SNMP MIB.

6. The trap message is sent by the management agent to the managing entity (and requires no response from the managing entity). A request-response message is sent by the managing entity, with the response coming back from the management agent.

7. GetRequest, GetNextRequest, GetBulkRequest, SetRequest, InformRequest, Response, Trap

8. The SNMP engine is the part of an SNMP implementation that handles the dispatching, processing, authentication, access control, and timeliness of he SNMP messages. See Figure 8.5.

R12. What is meant by TLV encoding?

12. In TLV encoding, each piece of data is tagged with its type, length, and value.

TLV;
Type
Length
Value

Chapter 8: Network Security

Potential Questions

R3. From a service perspective, what is an important difference between a symmetric-key system and a public-key system?

R4. Suppose that an intruder has an encrypted message as well as the decrypted version of that message. Can the intruder mount a ciphertext-only attack, a known-plaintext attack, or a chosen-plaintext attack?

4. In this case, a known plaintext attack is performed. If, somehow, the message encrypted by the sender was chosen by the attacker, then this would be a chosen-plaintext attack.

5. An 8-block cipher has 2^8 possible input blocks. Each mapping is a permutation of the 2^8 input blocks; so there are $2^8!$ possible mappings; so there are $2^8!$ possible keys.

3. One important difference between symmetric and public key systems is that in symmetric key systems both the sender and receiver must know the same (secret) key. In public key systems, the encryption and decryption keys are distinct. The encryption key is known by the entire world (including the sender), but the decryption key is known only by the receiver.

R5. Consider an 8-block cipher. How many possible input blocks does this cipher have? How many possible mappings are there? If we view each mapping as a key, then how many possible keys does this cipher have?

R7. Suppose $n = 10{,}000$, $a = 10{,}023$, and $b = 10{,}004$. Use an identity of modular arithmetic to calculate in your head $(a \bullet b) \bmod n$.

R8. Suppose you want to encrypt the message 10101111 by encrypting the decimal number that corresponds to the message. What is the decimal number?

7. a mod n = 23 , b mod n = 4. So (a*b) mod n = 23*4=92

8. 175

P8. Consider RSA with $p = 5$ and $q = 11$.

a. What are n and z?

b. Let e be 3. Why is this an acceptable choice for e?

c. Find d such that $de = 1 \pmod z$ and $d < 160$.

d. Encrypt the message $m = 8$ using the key (n, e). Let c denote the corresponding ciphertext. Show all work. *Hint:* To simplify the calculations, use the fact:

$$[(a \bmod n) \bullet (b \bmod n)] \bmod n = (a \bullet b) \bmod n$$

Problem 8

p = 5, q = 11

a) n = p*q = 55, z = (p-1)(q-1) = 40

b) e = 3 is less than n and has no common factors with z.

c) d = 27

d) m = 8, me = 512, Ciphertext c= me mod n = 17

m üzeri e yani 8^3 = 512, c = 512 mod 55 = 17

1. to encrypt message m ($<n$), compute

$c = m^e \bmod n$

2. to decrypt received bit pattern, c, compute

$m = c^d \bmod n$

Chapter 6: Wireless and Mobile Networks

No question…

Chapter 5: Link layer

R4. Suppose two nodes start to transmit at the same time a packet of length L over a broadcast channel of rate R. Denote the propagation delay between the two nodes as d_{prop}. Will there be a collision if $d_{prop} < L/R$? Why or why not?

R5. In Section 5.3, we listed four desirable characteristics of a broadcast channel. Which of these characteristics does slotted ALOHA have? Which of these characteristics does token passing have?

R6. In CSMA/CD, after the fifth collision, what is the probability that a node chooses $K = 4$? The result $K = 4$ corresponds to a delay of how many seconds on a 10 Mbps Ethernet?

4. There will be a collision in the sense that while a node is transmitting it will start to receive a packet from the other node.

5. Slotted Aloha: 1, 2 and 4 (slotted ALOHA is only partially decentralized, since it requires the clocks in all nodes to be synchronized). Token ring: 1, 2, 3, 4.

6. After the 5th collision, the adapter chooses from {0, 1, 2,…, 31}. The probability that it chooses 4 is 1/32. It waits 204.8 microseconds.

R9. How big is the MAC address space? The IPv4 address space? The IPv6 address space?

9. 2^{48} MAC addresses; 2^{32} IPv4 addresses; 2^{128} IPv6 addresses.

R15. What is the maximum number of VLANs that can be configured on a switch supporting the 802.1Q protocol? Why?

15. In 802.1Q there is a 12- bit VLAN identifier. Thus 2^{12} = 4,096 VLANs can be supported.

P17. Recall that with the CSMA/CD protocol, the adapter waits $K \cdot 512$ bit times after a collision, where K is drawn randomly. For $K = 100$, how long does the adapter wait until returning to Step 2 for a 10 Mbps broadcast channel? For a 100 Mbps broadcast channel?

Problem 17

Wait for 51,200 bit times. For 10 Mbps, this wait is

$$\frac{51.2 \times 10^3 \, bits}{10 \times 10^6 \, bps} = 5.12 \, \text{msec}$$

For 100 Mbps, the wait is 512 μ sec.

Chapter 1, 2, 3 ve 4

R8. Three types of switching fabrics are discussed in Section 4.3. List and briefly describe each type. Which, if any, can send multiple packets across the fabric in parallel?

8. Switching via memory; switching via a bus; switching via an interconnection network. An interconnection network can forward packets in parallel as long as all the packets are being forwarded to different output ports.

Q2)

R20. Look over your received emails, and examine the header of a message sent from a user with an .edu email address. Is it possible to determine from the header the IP address of the host from which the message was sent? Do the same for a message sent from a gmail account.

A2)

20. You should be able to see the sender's IP address for a user with an .edu email address. But you will not be able to see the sender's IP address if the user uses a gmail account.

Q3)

R12. Do routers have IP addresses? If so, how many?

R13. What is the 32-bit binary equivalent of the IP address 223.1.3.27?

A3)

12. Yes. They have one address for each interface.

13. 11011111 00000001 00000011 00011100.

Q4)

R19. Compare and contrast the IPv4 and the IPv6 header fields. Do they have any fields in common?

R20. It has been said that when IPv6 tunnels through IPv4 routers, IPv6 treats the IPv4 tunnels as link-layer protocols. Do you agree with this statement? Why or why not?

A4)

ipv6 has more address space and fixed length header constract to ipv4

Ipv4	Ipv6
IPv4 is a 32-bit address.	IPv6 is a 128-bit address.
IPv4 is a numeric address that consists of 4 fields which are separated by dot (.).	IPv6 is an alphanumeric address that consists of 8 fields, which are separated by colon.
IPv4 has 5 different classes of IP address that includes Class A, Class B, Class C, Class D, and Class E.	IPv6 does not contain classes of IP addresses.
IPv4 has a limited number of IP addresses.	IPv6 has a large number of IP addresses.

19. IPv6 has a fixed length header, which does not include most of the options an IPv4 header can include. Even though the IPv6 header contains two 128 bit addresses (source and destination IP address) the whole header has a fixed length of 40 bytes only. Several of the fields are similar in spirit. Traffic class, payload length, next header and hop limit in IPv6 are respectively similar to type of service, datagram length, upper-layer protocol and time to live in IPv4.

20. Yes, because the entire IPv6 datagram (including header fields) is encapsulated in an IPv4 datagram.

Q5)

R26. In Section 2.7, the UDP server described needed only one socket, whereas the TCP server needed two sockets. Why? If the TCP server were to support *n* simultaneous connections, each from a different client host, how many sockets would the TCP server need?

A5)

26. With the UDP server, there is no welcoming socket, and all data from different clients enters the server through this one socket. With the TCP server, there is a welcoming socket, and each time a client initiates a connection to the server, a new socket is created. Thus, to support n simultaneous connections, the server would need *n+1* sockets.

Q6)

R4. Describe why an application developer might choose to run an application over UDP rather than TCP.

R5. Why is it that voice and video traffic is often sent over TCP rather than UDP in today's Internet? (*Hint*: The answer we are looking for has nothing to do with TCP's congestion-control mechanism.)

R6. Is it possible for an application to enjoy reliable data transfer even when the application runs over UDP? If so, how?

A6)

4. An application developer may not want its application to use TCP's congestion control, which can throttle the application's sending rate at times of congestion. Often, designers of IP telephony and IP videoconference applications choose to run their applications over UDP because they want to avoid TCP's congestion control. Also, some applications do not need the reliable data transfer provided by TCP.

5. Since most firewalls are configured to block UDP traffic, using TCP for video and voice traffic lets the traffic though the firewalls.

6. Yes. The application developer can put reliable data transfer into the application layer protocol. This would require a significant amount of work and debugging, however.