Problems and Solutions (Chapter 9)

1. From a local wireless service provider, find out what kind of EIR information is retained for each subscriber?

   [Solution]

   Cingular is using GSM, and GSM use IMEI (International Mobile Equipment Identifier) as EIR information.

2. You have temporarily moved to a new area and you would like to use your cell phone. What alternatives do you have if:

   (a) There is no service provider in that area?

   (b) There is no agreement between your wireless phone service provider and the service provider in the new area?

   (c) The area is covered only by a satellite phone service?

   [Solution]

   (a) It is impossible to use a cell phone where no service provider (including satellite phone service) exists.

   (b) If there is no agreement, there is nothing you can do in the new area. You can register your cell phone to the new service provider in the new area, if that employs the same technology and reprogrammed for new frequency band and/or code.

   (c) Subscribe your cell phone to a satellite phone service provider, if it is capable to use the satellite frequency band.

3. What is the bandwidth and the power level used by the "beacon signals" in your area?

   [Solution]

   GSM use $1850 - 1910$ MHz for beacon signals, therefore the bandwidth is 60 MHz.

4. Like the cellular system, the IEEE 802.11 wireless LANs also have the "beacon signals". Search for an IEEE 802.11 specification online and find out what information are included in a beacon signal.

   [Solution]

   See the IEEE 802.11 standard.

5. From your favorite web site, find out the acceptable bit error rate for the following applications:

   (a) Voice communication

   (b) Video communication

(c) Defense applications

(d) Sensor data communication in a nuclear plant

(e) Sensor measuring paper thickness in a plant

(f) Sensor measuring temperature for different parts of a chemical process

(g) Sensor measuring accuracy of a lathe machine

[Solution]

To be done by student.

6. Asssuming that you just got out of the airplane and you switched on your cell phone. If the closest BS is located at a distance of 5 kms, what is the minimum and the maximum delay before a contact is established between your cell phone and the nearest BS, given the BS transmits beacon signals every one second?

   [Solution]

   The registration process including:

   T_1: Beacon signal exchange between BS and MS

   T_2: MS request for registration

   T_3: Visiting BS send authentication request to home BS

   T_4: Home BS send authentication response back to the visiting BS

   T_5: Visiting BS send the authentication/rejection back to MS

   Suppose T_3 and T_4 are fixed, then the minimum delay is

   $$T_2 + T_3 + T_4 + T_5 = 2 * (\frac{5 \text{ km}}{3 * 108}) + T_3 + T_4,$$

   and the maximum delay is

   $$1 + T_1 + T_2 + T_3 + T_4 + T_5 = 1 + 3 * (\frac{5 \text{ km}}{3 * 108}) + T_3 + T_4.$$

7. In the backbone network, it is desirable to find out the shortest path from the source to the destination. How do you do this in a wireless network environment, where the subscribers do have finite mobility? Explain clearly.

   [Solution]

   In a wireless network, a HA (home agent) and FA (foreign agent) can be used to deal with the mobility. If the subscribers have finite mobility, the HA and FA are able to cooperate with each other to locate the subscriber. When a source want to send a message to a destination and the HA has the current location information of the destination, then the message can be delivered to a destination subscriber along the shortest path as in the backbone network.

8. What is the use of "attachment points" from one network to another network? Explain its significance in wireless network routing?

   [Solution]

   They are the gateway routers which route the packets into/out of one network to another network. Gateway routers support routing within backbone.

9. In a wireless network, the radio signal is broadcast through the air. Therefore, what is the significance of multicasting in this context? Explain in detail.

   [Solution]

   When a wireless network use a common channel, only stations in the radio range of the sender can receive the signal. Multicasting implies formation of group members beyond the radio range so that all can receive intended message.

10. What is meant by bidirectional tunneling? Why do you need HA-FA in addition to HLR-VLR pair? Explain clearly.

    [Solution]

    The bidirectional tunneling approach is that when an MS moves into a foreign network, a binding update is sent to the HA, which then responses with a binding acknowledgement. After that, a bidirectional tunnel is created by HA to the FA that is currently serving the MS and HA encapsulates the packets for the MS.

11. The function of a 10×10 permutator is given by the following table:

Input	1	2	3	4	5	6	7	8	9	10
Output	1	6	2	7	3	8	4	9	5	10

    Find out the output message going through the air if the input message sequence is given by:

    I WANT TO LEARN ABOUT PERMUTATION FUNCTION IN WIRELESS DEVICES AND APPLICATIONS....

    Assume that the message is transmitted as a group of ten characters.

    [Solution]

    Input:

1	2	3	4	5	6	7	8	9	10
I		W	A	N	T		T	O	
L	E	A	R	N		A	B	O	U
T		P	E	R	M	U	T	A	T
I	O	N		F	U	N	C	T	I
O	N		I	N		W	I	R	E
L	E	S	S		D	E	V	I	C
E	S		A	N	D		A	P	P
L	I	C	A	T	I	O	N	S	

Output after permutation:

1	2	3	4	5	6	7	8	9	10
I	T			W	T	A	O	N	
L		E	A	A	B	R	O	N	U
T	M		U	P	T	E	A	R	T
I	U	O	N	N	C		T	F	I
O		N	W		I	I	R	N	E
L	D	E	E		V	S	I		C
E	D	S			A	A	P	N	P
L	I	I	O	C	N	A	S	T	

Therefore, the output is:

IWN O ATT LANAOER BUTPRUA EMTTINFNTO UCIO NWRNI IELS EIESDVCE N PSADAPLCTOSIAIN

12. Consider the word "wireless" comprised of 8 symbols, each symbol being a letter of the English alphabet.This word is encrypted by first applying a permutation function and then a substitution function. The permutation function is applied on a 4 symbol half word as follows: (1234) => (4132), i.e. every half word with input symbols 1234 is transformed to an output half word, which is 4132. The word is interpreted as a sequence of 2 half words. The substitution function is as follows:

Input Symbol:	w	i	r	e	l	s
Output Symbol:	i	r	e	l	s	w

(a) What is the final output?

(b) What would be the output if the substitution function were applied before the permutation function instead of after it?

[Solution]

(a)

Original	w	i	r	e	l	e	s	s
After permutation	e	w	r	i	s	l	s	e
After substitution	l	i	e	r	w	s	w	l

The output is "lierwswl".

Original	w	i	r	e	l	e	s	s
After permutation	i	r	e	l	s	l	w	w
After substitution	l	i	e	r	w	s	w	l

The output is "lierwswl".

13. The function of an 8×8 permutator is given by the following table:

Input	1	2	3	4	5	6	7	8
Output	8	4	2	1	7	5	3	6

The following message is to be sent through the air:

I AM DONE WITH MY FINALS AND NOW CAN TAKE A BREAK OR A VACATION.

Find the message going through the air if

(a) An 8-way interleaving is done before using the permutator

(b) If an 8-way interleaving is done after using a permutator and before it is transmitted

[***Solution***]

Organizing a group of 8-characters together, the given text:

I AM DONE WITH MY FINALS AND NOW CAN TAKE A BREAK OR A VACATION.

is converted as:

I		A	M		D	O	N
E		W	I	T	H		M
Y		F	I	N	A	L	S
	A	N	D		N	O	W
	C	A	N		T	A	K
E		A		B	R	E	A
K		O	R		A		V
A	C	A	T	I	O	N	.

a. Interleaving gives

L	E	Y			E	K	A
			A	C			C
A	W	F	N	A	A	O	A
M	I	I	D	N		R	T
	T	N			B		I
D	H	A	N	T	R	A	O
O		L	O	A	E		N
N	M	S	W	K	A	V	.

and the text as:

IEY EKA AC CAWFNAAOAMIIDN RT TN B IDHANTRAOO LOAE NNMSWKAV.

Doing permutation as per the permutation table gives:

	Y	K	E	E	A		I
A					C	C	
N	F	O	W	A	A	A	A
D	I	R	I		T	N	M
	N		T	B	I		
N	A	A	H	R	O	T	D
O	L			E	N	A	O
W	S	V	M	A	.	K	N

and the text as:

YKEEA IA CC NFOWAAAADIRI TNM N TBI NAAHROTDOL ENAOWSVMA.KN

b. Doing permutation first gives:

M	A	O		D	N		I
I	W			H	M	T	E
I	F	L		A	S	N	Y
D	N	A	A	N	W		
N	A	O	C	T	K		
	A	E		R	A	B	E
R	O			A	V		K
T	A	N	C	O	.	I	A

Permutated output is:

MAO DN IIW HMTEIFL ASNYDNAANW NAOCTK AE RABERO AV KTANCO.IA

Doing interleaving gives:

M	I	I	D	N		R	T
A	W	F	N	A	A	O	A
O		L	O	A	E		N
			A	C			C
D	H	A	N	T	R	A	O
N	M	S	W	K	A	V	.
	T	N			B		I
I	E	Y			E	K	A

Permutation + Interleaving gives the output as:

MIIDN RTAWFNAAOAO LOAE N AC CDHANTRAONMSWKAV. TN B IIEY EKA

14. In RSA algorithm, the public key is transmitted to all MSs through the air by the BS. Then, how is the security ascertained?

[Solution]

Unlike in the classic symmetrical key cryptosystem with a single key being used for both encryption at the sender and decryption at the receiver, RSA algorithm has a pair of different keys, one is public key and the other is private key. A message encrypted by the public key only can be decrypted by the corresponding private key. As long as the private key is kept secret, even though the public key of a MS is known by others, the BS still can authenticate a MS securely.

15. Given two prime numbers, $p = 37$ and $q = 23$, define the private and public keys by selecting appropriate value of the number "e"?

[Solution]

(a) $N = p * q = 37 * 23 = 851$

$PHI = (p-1)(q-1) = 792$

The public exponent e will be generated so that the greater common divisor of e and PHI is 1. In other words, e is relatively prime with PHI.

$e = 5$

The public key is $(n, e) = (851, 5)$

The private key $(d) = (317)$ to satisfy that $(ed - 1)$ is dividable by PHI.

(b) The private key $(d) = (317)$ to satisfy that $(ed - 1)$ is dividable by PHI.

16. Answer the following:

(a) Using the public key of Problem 11, find the sequence of values transmitted through the air if the ASCII values corresponding to the following message is sent by the BS:

I LIKE THIS CLASS.

(b) Verify, how this message is recovered back at the MS, by using the public key.

[Solution]

(a)

Original	ASCII (hex)	ASCII (dec)	C
I	49	73	702
	20	32	353
L	4C	76	661
I	49	73	702
K	4B	75	186
E	45	69	575
	20	32	353
T	54	84	766
H	48	72	634
I	49	73	702
S	53	83	774
	20	32	353
C	43	67	842
L	4C	76	661
A	41	65	632
S	53	83	774
S	53	83	774
.	2E	46	552

(b)

Code	ASCII (dec)	ASCII (hex)	Decrypted
702	73	49	I
353	32	20	
661	76	4C	L
702	73	49	I
186	75	4B	K
575	69	45	E
353	32	20	
766	84	54	T
634	72	48	H
702	73	49	I
774	83	53	S
353	32	20	
842	67	43	C
661	76	4C	L
632	65	41	A
774	83	53	S
774	83	53	S
552	46	2E	.

17. Answer the following:

    (a) How do you differentiate between privacy and security?

    (b) What are the differences between authentication and encryption?

[Solution]

(a) Privacy is something that will only interest "those with something to hide". Security is a necessary tool to build privacy, but a communication or transaction environment can be very secure, yet totally unprivate.

Security and privacy are closely related technologies, however, there are important differences that need to be understood in order to design new systems that address both. Privacy is about informational self-determination (i.e., the ability to decide what information about goes where).

Security offers the ability to be confident that those decisions are respected. For example, we talk about GSM voice privacy – can someone listen to my call? There is a privacy goal, which is to allow me to say no, and a security technology, encryption, that allows me to enforce it. In this example, the goals of security and privacy are the same. But there are other times when they may be orthogonal, and there are also times when they are in conflict.

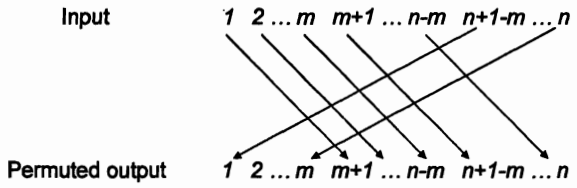

Figure 1: Figure of problem 9.20.

(b) Encryption is the process of hiding the data that others canot understand. While authentication is to grant or remove the right for others to access the data.

18. Why do you need to send a random number to test a MS? Explain clearly.

[Solution]

To avoid fixed bit pattern which can possibly be retained and replayed by malicious users.

19. Answer the following:

(a) Do you recall any recent event that is an example of denial of service?

(b) Can DoS (Denial of Service) be more effective if you have information about the traffic? Explain clearly.

[Solution]

Sometimes we cannot access some web sites. If we know the information about the traffic and realize that the traffic is too high, we can use Denial of Service (DoS) to reject some user's request and provide service for others. This happened many Internet service providers including AOL, just few years ago.

20. A linear permutation $i \rightarrow (i+m) \bmod n$ is used as follows: Does the encryption depends on thevalue of m? What is the impact of increasing the value of m? Explain clearly.

[Solution]

The encryption depends on the value of m since it decides how many bits shift in the output. As the value of m is increased, the number of bits shift in the output is increasing too. When $m > n$, then v should not be a multiple of m, since the output will be exactly the same as the input in this case.

21. In organizing a conference, a single key has to be used by all program committee members to encrypt and decrypt the message. Sssuming this

key has be changed every year, how can you set up such a "session key" using public-private key pairs? Explain clearly.

[Solution]

The organizer of the conference should generate a public-private key pair for each member and assign the private key to a corresponding member off line or personally. Once the session key needs to be setup or changed, the organizer encrypts the new session key by each member's public key and sends it to the corresponding member. Each member uses its private key to decrypt the received message and obtain the new session key, which will be the same for all members; but the encrypted session key is different for each user.