Name: Chen Hao Cheng
Cyber Security: HW2

Review Question

2.4) List three approaches to message authentication.

Message Authentication is a procedure that allows communication parties to verify that received or stored message authentic.

1. Authentication Using Symmetric Encryption
    - Symmetric encryption is used to offer confidentiality for data that is transmitted or stored
    - On sender side, plain text and secret is given as inputs to the encryption algorithm and then produce the cipher text
    - On Receiver side, the decryption algorithm does the reverse operation of encryption algorithm by taking the cipher text and same secret key as input and produces the plain text as output
    - Symmetric encryption is not suitable for message authenticate
2. Message Authentication Code (MAC)
    - MAC is an authentication technique which produces MAC based on the message and the secret key using the algorithm
    - MAC is appended to the message at sender side when transmitting
    - On sender receiver side, the receiver receives the message with MAC, then only the message with the secret key is inputted to MAC algorithm and produce the MAC
    - MAC compare to check for message authentication
    - If both MAC are the same, then the receiver can ensure the message is from authentication sender without any modification
3. Secure Hash Function
    - Hash function is an authentication technique that accepts the message in variable length and produces the messages digest in fixed size as output
    - The message digest is appended to the message at sender side while transmitting
4. Other applications of hash functions

2.7) What properties must a hash function have to be useful for message authentication?

1) The block can have any size of block of data
2) The output can produce fixed-length
3) The hash function, H(x) is relative easy to compute for any given input x. Therefore, H(x) can be computed in a way such that it makes implementation of software and hardware more practical because H(x) can be any size.
4) One way or pre-image resistant. It should be infeasible to find the value of x by using hash code of h such that $H(x) = h$
5) It also should be infeasible computationally to find $y \neq x$ such that $H(y) = H(x)$. This is called second pre-image or weak collision resistant property. This property ensure that alternate message cannot be found using the same hash value.

6) It should be feasible to find any pair message (x, y) such that H(x) = H(y). This is called Collision resistant or strong collision resistance.

Problems

2.1)

Yes, there is a flaw in this scheme. Suppose the sender creates the random bit string 1001 (public) with secret key 0001, and XOR both to get 1000. And then send 1000 to the receiver, the receiver gets the outcome 1000, and the receiver XOR it with its secret key 0001, the receiver can get the random bit 1001 back. However, the hacker(eavesdropper) can get the outcome 1000 from sender while sending to the receiver, and the hacker can get the random bit string (which in this case, I'm assuming it is public), if the hacker XOR both, the hacker can inference the secret key which is 0001.

2.2a)

The redundant letters: the spaces and punctuations are omitted. So the first key is cryptographic, which the redundant of that is cryptogahi, containing 10 letters. If we put the message into a matrix, omit the spaces and punctuations, we would get:

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

Luckily, we got 10 X 10 matrix.

Next, we consider alphabetic order for "cryptogahi", which is a,c,g,h,i,o,p,r,t,y corresponding to 1,2,3,4,5,6,7,8,9,10. Meaning a = 1^{st}, c = 2^{nd} , g = 3^{rd} …so on. This is the reading order for later on.

We have

1	2	3	4	5	6	7	8	9	10
C	R	Y	P	T	O	G	A	H	I

Since A is the first to read which is column 8 from the first matrix, and C is the second to read from the first matrix, which is column 1, and keep doing this until all letters are done, then we would get the message as we read from top to bottom:

"trfhe hftin brouy rtust eaeth gisre hftea tyrnd irolt aougs hllet inibi tihiu oveuf edmtc esatw tledm nedlr aptse terfo"

And we can do it again for another key, “network security”. The redundant letters of it is “networkscuiy”, but this contains 12 letters. We can make it 10 because the first key is 10 letters after doing redundant letters. Thus, we get “networkscu” and we make another matrix based off the new message we got:

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

Next, we consider the alphabetic order for “networkscu”, which is “c, e, k, n, o, r, s, t, u, w” corresponding to 1 to 10. Meaning c = 1^{st} , e = 2^{nd} , k = 3^{rd} … so on.

1	2	3	4	5	6	7	8	9	10
N	E	T	W	O	R	K	S	C	U

Since C is the first to read from alphabetic order, which is column 9, and then E is the second in column 2 and so on, we will get a message:

“isrng butlf rrafr lidlp ftiyo nvsee tbehi hteta eyhat tucme hrgta ioent tusru ieadr foeto lhmet nteds ifwro hutel eitds”