CIS4367.01 **Brandon Thompson**

Prof. Elibol Due Date: 1/27/20

Homework 3

PROBLEM 2.1:

Suppose that someone suggests the following way to confirm that the two of you are both in possession of the same secret key. You create a random bit string the length of the key, and send the result over the channel. Your partner XORs the incoming block with the key, and sends it back. You check, and if what you receive is your original random string, you have verified that your partner has the same secret key, yet neither of you has ever transmitted the key. Is there a flaw in this scheme?

SOLUTION:

Yes, because the random bit string and the XORed value are both transferred over the network, if someone was listening on the communication and got both of these values, the XOR of the two would be the secret key.

PROBLEM 2.2:

This problem uses a real-world example of a symmetric cipher, from an old U.S. Special Forces manual (public domain). The document, filename *Special Forces.pdf*, is available at `box.com/CompSec3e`.

a Using the two keys (memory words) *cryptographic* and *network security*, encrypt the following message:

Be at the third pillar from the left outside the lyceum theatre tonight at seven. If you are distrustful bring two friends.

Make reasonable assumptions about how to treat redundant letters and excess letters in the memory words and how to treat spaces and punctuation. Indicate what your assumptions are.
Note: The message is from the Sherlock Holmes novel *The Sign of Four*.

b Decrypt the ciphertext. Show your work.

c Comment on when it would be appropriate to use this technique and what its advantages are.

SOLUTION:

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

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

Ciphertext:
UIXTT EHDTX NRBEO LINOC DTXRH ELOTS ISYTX RFDXI UTEPE UEFIX WUFET
HYTTR HXGTU EETGA LLIEN TRFRE XRBAV EMSFS RXATI MLADH OAHXI TOSNE

Number of letters: 110
Size of keyword: 10
Number of rows: $\frac{110}{10} = 11$
Write ciphertext into columns based on order defined by the second memory word.
Transpose the rows into the columns defined by the first memory word.

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

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

Plaintext:
Be at the third pillar from the left outside the lyceum theatre tonight at seven. If you are distrustful bring two friends.

PROBLEM 2.5:

In this problem we will compare the security services that are provided by digital signatures (DS) and message authentication codes (MAC). We assume that Oscar is able to observe all messages sent from Alice to Bob and vice versa. Oscar has no knowledge of any keys but the public one in case of DS. State whether and how (i) DS and (ii) MAC protect against each attack. The value auth(x) is computed with a DS or a MAC algorithm, respectively.

a (Message integrity) Alice sends a message $x =$ ″Transfer $1000 to Mark″ in the clear and also sends auth(x) to Bob. Oscar intercepts the message and replaces ″Mark″ with ″Oscar.″ Will Bob detect this?

b (Replay) Alice sends a message $x =$ ″Transfer $1000 to Oscar″ in the clear and also sends auth(x) to Bob. Oscar observes the message and signature and sends them 100 times to Bob. Will Bob detect this?

c (Sender authentication with cheating third party) Oscar claims that he sent some message x with a valid auth(x) to Bob but Alice claims the same. Can Bob clear the questions in either case?

d (Authentication with Bob cheating) Bob claims that he received a message x with a valid signature auth(x) from Alice (e.g., ″Transfer $1000 from Alice to Bob″) but Alice claims that she never sent it. Can Alice clear this question in either case?

SOLUTION:

a Will be detected by both (i) DS and (ii) MAC.

b Will **not** be detected by either (i) DS or (ii) MAC, unless a time-stamp is added.

c (i) DS: Bob has to verify the message with the public key from both. Only Alice's public key will give a valid verification.
(ii) MAC: Bob has to receive the secret key from Alice and Bob (he already has these) and verify which message has the proper auth(x).

d (i) DS: Alice has to receive a copy of the message with the signature. Then Alice can show that message and signature can be verified with Bob's public key. Meaning Bob must have generated the message. (ii) MAC: No, Bob can say that Alice generated this message.

PROBLEM 2.6:

Suppose $H(m)$ is a collision-resistant hash function that maps a message of arbitrary bit length into an n-bit hash value. Is it true that, for all messages x, x' with $x \neq x'$, he have $H(x) \neq H(x')$? Explain your answer.

SOLUTION:
Every hash function with more inputs than outputs will theoretically have collisions. The pigeonhole principle guarantees that some inputs will hash to the same outputs.
Collision resistance does not mean that no collisions exist, only that they are harder to find.
Birthday paradox states that if an function produces N bits of output, an attacker who computes $2^{\frac{N}{2}}$ hashes will find a pair that matches.

PROBLEM 2.8:

Prior to the discovery of any specific public-key schemes, such as RSA, an existence proof was developed whose purpose was to demonstrate that public key encryption is possible in theory. Consider the functions $f_1(x_1) = z_1$; $f_2(x_2, y_2) = z_2$; $f_3(x_3, y_3) = z_3$ where all values are integers with $1 \leq x_i, y_i, z_i \leq N$. Function f_1 can be represented by a vector **M1** of length N, in which the kth entry is the value of $f_1(k)$. Similarly, f_2 and f_3 can be represented by $N \times N$ matrices **M2** and **M3**. The intent is to represent the encryption/decryption process by table look-ups for tables with very large values of N. Such tables would be impractically huge but could, in principle, be constructed. The scheme works as follows: Construct **M1** with a random permutation of all integers between 1 and N; that is, each integer appears exactly once in **M1**. Construct **M2** so that each new row contains a random permutation of the first N integers. Finally, fill in **M3** to satisfy the following condition:

$$f_3\left(f_2\left(f_1(k), p\right), k\right) = p \forall k, p \text{ with } 1 \leq k, p \leq N$$

In words,

1. **M1** takes an input k and produces an output x.
2. **M2** takes inputs x and p giving output z.
3. **M3** takes inputs z and k and produces p.

The three tables, once constructed, are made public.

a It should be clear that it is possible to construct **M3** to satisfy the preceding condition. As an example, fill in **M3** for the following simple case:

$$\text{M1} = \begin{array}{|c|}\hline 5 \\ \hline 4 \\ \hline 2 \\ \hline 3 \\ \hline 1 \\ \hline \end{array} \quad \text{M2} = \begin{array}{|c|c|c|c|c|}\hline 5 & 2 & 3 & 4 & 1 \\ \hline 4 & 2 & 5 & 1 & 3 \\ \hline 1 & 3 & 2 & 4 & 5 \\ \hline 3 & 1 & 4 & 2 & 5 \\ \hline 2 & 5 & 3 & 4 & 1 \\ \hline \end{array} \quad \text{M3} = \begin{array}{|c|c|c|c|c|}\hline 5 & & & & \\ \hline 1 & & & & \\ \hline 3 & & & & \\ \hline 4 & & & & \\ \hline 2 & & & & \\ \hline \end{array}$$

Convention: The ith element of **M1** corresponds to $k = i$. The ith row of **M2** corresponds to $x = i$; the jth column of **M2** corresponds to $p = j$. The ith row of **M3** corresponds to $z = i$; the jth column of **M3** corresponds to $k = j$. We can look at this in another way. The ith row of **M1** corresponds to the ith column of **M3**. The value of the entry in the ith row selects a row of **M2**. The entries in the selected **M3** column are derived from the entries in the selected **M2** row. The first entry in the **M2** row dictates where the value 1 goes in the **M3** column. The second entry in the **M2** row dictates where the value 2 goes in the **M3** column, and so on.

b Describe the use of this set of tables to perform encryption and decryption between two users.

c Argue that this is a secure scheme.

SOLUTION:

a M3 =

5	2	4	1	5
1	4	2	3	2
3	1	5	2	3
4	3	1	4	4
2	5	3	5	1

b Bob selects random numbers to use as his private and public key. Sends the key to Alice. Alice encrypts the messages using Bobs public key, and the **M2** table. Bob can decrypt this using the **M1** and **M3** tables.

c The table used could be very large with random numbers as the inputs. This will give greater security and be infeasible to reverse engineer the tables in a acceptable amount of time.