INF140-Introducation to Cybersecurity

Mandatory Assignment 1: 100 pts in 5 pages
*Deadline: **September 26**, 2021*

Overview of Cybersecurity (15 pts)

Read through Chapter 1 and work on the following questions.

Question 1. Explain the meanings of the following security attributes in computer systems: confidentiality, integrity, authenticity, accountability, availability. (5 pts)

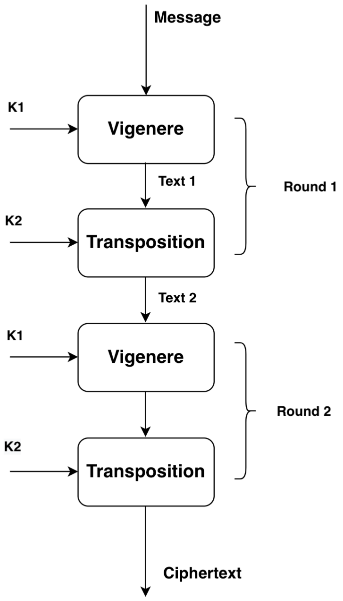
Question 2. List and briefly define the kinds of threat consequences and the types of threat action that cause these consequences. (5 pts)

Question 3. Refer to Figure 1.2 Security Concepts and Relationships in Section 1.1 in Chapter 1. Think of an example that involves all blocks in the figure and go through the relations of entities and relevant techniques in your example. Draw a similar figure that consists of concrete entities, techniques, countermeasures. (5 pts)

Cryptographic Tools (60 pts)

Question 4. (*15 pts*)

The following toy cipher is a product of two weaker ciphers in two rounds (which uses a similar idea as in the design of many modern block ciphers)



As shown in the figure, the Vigenere cipher uses a secret key **K1** to encrypt the message, and the output Text 1 is fed to the (column) Transposition cipher with a secret key **K2**. The output of Round 1 is treated as the input of Round 2 that has the same structure and keys as Round 1. Finally, the output of Round 2 is the ciphertext.

Suppose the secret keys are **K1=jisuan** and **K2=3415726** and the message **M** is

Cybersecurity is actually determined by the weakest link

in the encryption of the toy cipher. You are aksed to:

- give the intermediate output Text 1 from the Vigenere cipher (3 pts);
- give the intermediate output Text 2 from the Transposition cipher (3 pts);
- give the final ciphertext (3 pts); and

Suppose you're the recipient of the ciphertext, and you knew the cipher design, secret keys **K1** and **K2** in advance. Demonstrate the decryption on the ciphertext, and compare the output of your decryption operation with the original message. (6 pts)

Hint: refer to http://practicalcryptography.com/ciphers/ for the above ciphers and the space is to be removed in encryption.
NB: a submission simply with ciphertexts is not sufficient; your solution must demonstrate that you are able to carry out both encryption and decryption correctly either by manual calculations or by programming in Python.

Question 5. (*20 pts*)

This problem introduces a hash function similar in spirit to SHA-1 that operates on letters instead of binary data. It is called the toy tetragraph hash (TTH). Given a message consisting of a sequence of letters, TTH produces a hash value consisting of four letters. First, TTH divides the message into blocks of 16 letters, ignoring spaces, punctuation, and capitalization. If the message length is not divisible by 16, it is padded out with nulls. A four-number running total is maintained that starts out with the value (0, 0, 0, 0); this is input to a function, known as a compression function, for processing the first block. The compression function consists of two rounds:

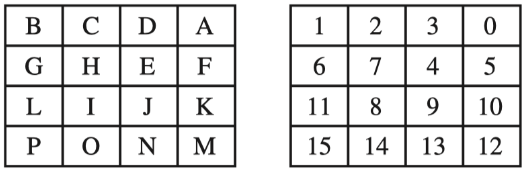
Round 1. Get the next block of text and arrange it as a row-wise 4×4 block of text and convert it to numbers ($A = 0$, $B = 1, \ldots, Z = 25$), for example, for the block ABCDEFGHIJKLMNOP, we have

A	B	C	D
E	F	G	H
I	J	K	L
M	N	O	P

0	1	2	3
4	5	6	7
8	9	10	11
12	13	14	15

Then, add each column mod 26 and add the result to the running total, mod 26. In this example, the running total is $(24, 2, 6, 10)$.

Round 2. Using the matrix from round 1, rotate the first row left by 1, second row left by 2, third row left by 3, and reverse the order of the fourth row. In our example



B	C	D	A
G	H	E	F
L	I	J	K
P	O	N	M

1	2	3	0
6	7	4	5
11	8	9	10
15	14	13	12

Now, add each column modulo 26 and add the result to the running total. The new running total is (5, 7, 9, 11). This running total is now the input into the first round of the compression function for the next block of text. After the final block is processed, convert the final running total to letters. For example, if the message is ABCDEF-GHIJKLMNOP, then the hash is FHJL.

1. Draw figures of the overall TTH logic and the compression function logic (5 pts)
2. Calculate the hash function for the 48-letter message “He left twenty million US dollars to his beloved children." (7 pts)
3. To demonstrate the weakness of TTH, find a 48-letter block that produces the same hash as that just derived. (8 pts)

Question 6. (*15 pts*)

(1) Perform encryption and decryption using the RSA algorithm, as in the slides, for the following examples (9 pts: 3 pts for each):

1. $p = 3; q = 17, e = 5; M = 6$
2. $p = 5; q = 17, e = 7; M = 4$
3. $p = 7; q = 17, e = 29; M = 7$

(2) Suppose the word SECURITY is to be encrypted by RSA with parameters $p = 13; q = 19, e = 5$. What is the corresponding ciphertext in hexadecimal form? In this task you need to encode each letter to a number according to the ASCII table and use one byte to store the ciphertext of each letter. (6 pts)

Question 7. (*10 pts*)

After taking some courses on cryptography, Alice and Bob decide to try it out in their communication. They agree that they will use Vigenere cipher for data encryption/decryption, and RSA for sharing secrete key, where the key of Vigenere cipher only uses letters $A, B, \cdots, J$ and letters in a key are encoded as digits $0, \ldots, 9$ for RSA as

A	B	C	D	E	F	G	H	I	J
0	1	2	3	4	5	6	7	8	9

Alice chooses a RSA public key $(n, e) = (341, 7)$. Bob uses the Vigenere cipher to encrypt a sentence and encrypt the Vigenere key by Alice's RSA public key. For instance, Bob uses the Vigenere with the secret key CCG to encrypt certain message, and send the ciphertext together with the number $41 = 226^7 \mod 341$, where 226 is derived from the key CCG according to the lookup table.

Suppose Bob sends the following message to Alice:

82,
uhhgiyfmrtthgfldihotfzbhsdhgeqeeutaufaquifjpduiroegvcduirodhuefuirorhbcwjoqbng
sevjllfnffdrsepfmefrfzbhsshduujtbjspvcknouftkbndoiwuosjc.

Answer the following questions:

- What is the Vigenere key used by Bob? (5 pts)
- What is the original message from Bob? (5 pts)

User Authentication (25 pts)

Question 8. Suppose a computer system stores users' password by simply calculating the MD5 of "user name:password" and restricts password to chosen from lower case letters and digits with max. length 8.

1. Use OpenSSL to calculate the following user names and passwords (6 pts: 2 pts each):
   - Anaga:1234asdf
   - Maria:q1w2e3r4
   - Joseph:12345678

   Take a screenshot of your commands and results. (NB: Pay attention to the option of echo in your commands)
2. Use OpenSSL command to test the speed of MD5 in your computer. Suppose Nikolay is a user in the system, use the speed information to estimate how long do you need to crack Nikolay's password in the following cases (9 pts: 3 pts each):
   - Nikolay chooses a password of length 4 with all digits
   - Nikolay chooses a password of length 8 with all digits
   - Nikolay chooses a password of length 8, where each position either a digit or a lower-case letter

   In your answer, you should clearly give your estimation of the MD5 speed in your computer. For each case, you should show the steps how your estimation is obtained.

Question 9. The inclusion of the salt in the UNIX password scheme increases the difficulty of guessing by a factor of 4096. The salt is actually stored in plaintext in the same entry as the corresponding hashed password. Therefore, those two characters are known to the attacker and need not be guessed.

Why is it considered that the additional salt in the UNIX password scheme increases security? (4 pts)

Question 10. The following is an entry in the password file in a Linux system, which a root user can access (6 pts):

```
root:$6$Q8uKtWWm/dptau2a$E184j/HJuiuw2lsUT7yuBvTh3FioWj5KKUvPQT
  /1OJT4rtBACAm4NlEFV4n4x6ndTN3wD9A5uHOjEQQ/JJqN./:18142:0:99999:7:::
```

Search on the Internet and explain each segment in the above password.

Submission of your assignment

Instructions for your submission:

- Prepare your answers in the order of Questions 1 - 10 in a word file
- Take a screenshot of all your OpenSSL commands (Type your full name in the terminal and include it in your screenshot)
- If you have written codes for solving some questions, make sure your codes are properly commented and include your codes in your submission
- When you complete all your answers, save the word file as a PDF file.
- Compress the PDF file together with all other relevant files into a ZIP file. The name of the ZIP file should be in the format as INF140-MA1-*StudentID*, where the *StudentID* is your login ID. Finally upload the ZIP file to mittuib.no before the deadline.