IERG4130 Assignment 2

Q1: (5+5 points) Basic concepts of symmetric key encryption:

1. List a few applications of stream ciphers and block ciphers. At least 2 for each category.
2. Briefly explain the differences between stream ciphers and block ciphers.

Q2: (5+5 points) This problem explores the use of a one-time pad version of the Vigenère cipher. In this scheme, the key is a stream of random numbers between 0 and 26. For example, if the key is 3 19 5 ..., then the first letter of plaintext is encrypted with a shift of 3 letters, the second with a shift of 19 letters, the third with a shift of 5 letters, and so on.

1. Encrypt the plaintext *symmetric* with the key stream 9 0 1 7 23 15 21 14 11.
2. Using the ciphertext *keyencryption*, find a key so that the cipher text decrypts to the plaintext *secretsleaked*.

Q3: (10 points) Considering the RC4 algorithm: If the S-box is 4 bytes with 2-byte secrets 96 ($K[0] = 9$, $K[1] = 6$), then what is the plain text M for the 4-byte ciphertext *1234*? Show your process of calculation.

Q4: (5+5 points) Basic concepts of public key encryption:

1. What is the main assumption that makes RSA algorithm secure?
2. Why is CA (Certificate Authority) necessary for digital signatures?

Q5: (5+5 points) The following problems is about the calculation of RSA algorithms:

1. For a public-key encryption system based on RSA, if you observed a ciphertext C=9, and you know the receiver's public key is (e = 5, n = 35). Could you recover the corresponding plaintext M? Show your process of calculation.
2. In an RSA system, the public key of a given user is (e = 5, n = 33). Could you derive a possible private key for it? Show your process of calculation.

Q6: (5+5 points) Assume Alice and Bob are using Diffie-Hellman algorithm to create a secret key for AES. The chosen common prime number q is 11 and the primitive root a is 2.

1. If Alice's public key is 7, then what's a possible private key for Alice?
2. If Bob has the public key is 4, then what is the negotiated secrete key?

Q7: (2+3+5 points) Please open your browser and visit our department home page at: https://www.ie.cuhk.edu.hk. Inside the address bar, you will see a padlock icon just near the URL https://www..... and this means the website uses HTTPS to protect its traffic. It actually is built on digitally signed certificate.

1. Please get the X509 certificate file for this website (in pem format). You need to submit this file as your answer to this question.
2. That pem file was encoded. Please use openssl to decode it (for example: *openssl x509 -in www-ie-cuhk-edu-hk.pem -text -noout*). You may need to install *openssl* package/program on your computer. Save the output to a text file as part of your answer to this question.
3. What is the name of the issuer who has issued this certificate to IE department? What is the public key for that issuer?

Q8: (5+5 points) Basic concepts of message authentication code:

1. What is the advantage of HMAC (Keyed-Hashing for Message Authentication Code) over the hash functions without keys involved? Give an example (attack scenario) to explain it.
2. When a combination of symmetric encryption and an error control code is used for message authentication, in what order must the two functions be performed?

Q9: (5+5+10 points) This problem introduces a hash function similar in spirit to SHA that operations 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, example, for the block ABCDEFGHIJKLMNOP), we have 01234567891011121314 15 as following.

Round 1 Block in Letters	Round 1 Block in Numbers
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 row mod 26 and add the result to the running total (also need mod 26). In this example, the running total is $(6;22;12;2)$. Computation for $(6;22;12;2)$:

$$\begin{aligned}(0+1+2+3) \mod 26 &= 6 \mod 26 = 6\\ (4+5+6+7) \mod 26 &= 22 \mod 26 = 22\\ (8+9+10+11) \mod 26 &= 38 \mod 26 = 12\\ (12+13+14+15) \mod 26 &= 54 \mod 26 = 2\end{aligned}$$

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

Round 2 Block in Letters	Round 2 Block in Numbers
E J O P I N C L M B G H A F K D	4 9 14 15 8 13 2 11 12 1 6 7 0 5 10 3

Now, add each row mod 26 and add the result to the running total (the previous one $(6;22;12;2)$). The new running total is $(16;8;0;18)$. Computation for $(16;8;0;18)$:

$$\begin{aligned}((4+9+14+15) \mod 26 &= 42 \mod 26 = 16\\ (8+13+2+11) \mod 26 &= 34 \mod 26 = 8\\ (12+1+6+7) \mod 26 &= 26 \mod 26 = 0\\ (0+5+10+3) \mod 26 &= 18 \mod 26 = 18\end{aligned}$$

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, the message is "ABCDEFGHIJKLMNOP", then the hash is "WEMU". Computation for "WEMU":

$$((6;22;12;2)+(16;8;0;18)) \mod 26 = (22;30;12;20) \mod 26 = (22;4;12;20)$$

1. Draw figures of the overall TTH logic and the compression function logic.
2. Calculate the hash process for the 48-letter message, "THIS IS AN ASSIGNMENT FOR INTRODUCTION TO CYBERSECURITY".
3. To demonstrate the weakness of TTH, find a 48-letter block that produces the same hash as that just derived. (Hint: use lots of 'A's)

Change Log

1. IERG4130 F22 Assignment 2 Problems: The initial problem set.
2. IERG4130 F22 Assignment 2 Problems v2:
    1. Q3: Add more explanations such as "($K[0] = 9$, $K[1] = 6$)" and "4-byte ciphertext".
    2. Q9: Message changed from "IT IS AN ASSIGNMENT FOR INTRODUCTION TO CYBERSECURITY" to "THIS IS AN ASSIGNMENT FOR INTRODUCTION TO CYBERSECURITY".
3. IERG4130 F22 Assignment 2 Problems v3:
    1. Q8: Given the fact that HMAC is a kind of MAC, it should be HMAC vs. Hash instead of HMAC vs. MAC.
4. IERG4130 F22 Assignment 2 Problems v4:
    1. Q9: Pictures for Round 2 are corrected.