CS 558 Introduction to Computer Security, Spring 2024
Written Homework Assignment 1
Total points 125

Out: 2/28/2024 Wed.
Due: 3/11/2024 Mon. 23:59:59

---

1. (5 points) Encrypt the message:
we are all together
using a double transposition cipher with 4 rows and 4 columns, using the row permutation (1,2,3,4) => (2,4,1,3) and the column permutation (1,2,3,4) => (3,1,2,4).

A: The ciphertext is LEALETHRAWERGTOE. (lower case works too)

2. (15 points) An affine cipher is a type of simple substitution where each letter is encrypted according to the rule

$$c = (a * p + b) \mod 26$$

Here, p, c, a, and b are each numbers in the range 0 to 25, where p represents the plaintext letter, c the ciphertext letter, and a and b are constants. For the plaintext and ciphertext, 0 corresponds to "a" 1 corresponds to "b" and so on. Consider the ciphertext QJKES REOGH GXXRE OXEO, which was generated using an affine cipher. Determine the constants a and b and decipher the message. Hint: Plaintext "t" encrypts to ciphertext "H" and plaintext "o" encrypts to ciphertext "E." And suppose you know $5^{-1} \mod 26 = 21$ and $11^{-1} \mod 26 = 19$

A: We have that $7 = 19a + b(\mod 26)$ and $4 = 14a + b(\mod 26)$. Solving, we find the encryption function is $f(x) = 11x + 6(\mod 26)$ which implies the decryption function is $f^{-1}(x) = 19(x - 6)(\mod 26)$. The plaintext message is: if you bow at all bow low.

3. (15 points) Implement the A5/1 algorithm. Suppose that, after a particular step, the values in the registers are

$$X = (x0, x1, ..., x18) = (1010101010101010101)$$

$$Y = (y0, y1, ..., y21) = (1100110011001100110011)$$

$$Z = (z0, z1, ..., z22) = (11100001111000011110000)$$

List the next 5 keystream bits and give the contents of X, Y, and Z after these 5 bits have been generated.

A:10000

4. (15 points) Suppose that Trudy has a ciphertext message that was encrypted with the RC4 cipher. For RC4, the encryption formula is given by

$$c_i = p_i \oplus k_i$$

where k_i is the ith byte of the keystream, p_i is the ith byte of the plaintext, and c_i is the ith byte of the ciphertext. Suppose that Trudy knows the first ciphertext byte, and the first plaintext byte, that is, Trudy knows c_0 and p_0.

a) Show that Trudy can determine the first byte of the keystream k_0.
b) Show that Trudy can replace c_0 with c'$_0$, where c'$_0$ decrypts to a byte of Trudy's choosing, say, p'$_0$.
c) Suppose that a cryptographic integrity check is used (either a MAC, HMAC, or digital signature). Can Trudy's attack in part b still succeed? Explain.

A:
a. Trudy computes $k_0 = c_0 \oplus p_0$.
b. Replace c_0 with $p_0' \oplus k_0 = p_0' \oplus (c_0 \oplus p_0)$.
c. No. Any change in the ciphertext can be propagated into the MAC. Computes the MAC for the received message and then compare it with the received MAC to check if the integrity is violoated.

5. (10 points) Recall the attack on double DES. Suppose that we instead define double DES as C = D(E(P, K_1), K_2). Describe a meet-in-the-middle attack on this cipher.

A: It's the same as the "double DES" attack except that we must find K_1 and K_2 that satisfy E(C, K_2) = E(P, K_1).

6. (10 points) The formula for counter mode encryption is

$$C_i = P_i \oplus E(IV + i, K)$$

Suppose instead we use the formula

$$C_i = P_i \oplus E(K, IV + i)$$

Is this secure? If so, why? If not, why not?

A: No. The IV is not secret, so with a single block of known plaintext, Trudy can determine K and then decrypt all blocks.

7. (15 points) Suppose that Alice's RSA public key is (N, e) = (33, 3) and her private key is d = 7.
a) If Bob encrypts the message M = 19 using Alice's public key, what is the ciphertext C? Show that Alice can decrypt C to obtain M.
b) Let S be the result when Alice digitally signs the message M = 25. What is S? If Bob receives M and S, explain the process Bob will use to verify the signature and show that in this particular case, the signature verification succeeds.

A:
a) To encrypt: $19^3 = 28 \mod 33$. To decrypt: $28^7 = 19 \mod 33$.
b) The signed result is $S = M^d \mod N = 25^7 \mod 33 = 31$. To verify the signature, Bob computes $S^3 \mod N$ and the signature is verified if the result matches the received value

M. In this case, $31^3 = 25 \mod 33$. Assuming Bob receives the sent message M = 25, the signature is verified.

8. (10 points) Consider the Diffie-Hellman key exchange protocol. Suppose that Alice sends her Diffie-Hellman value, $g^a \mod p$, to Bob. Further, suppose that Bob wants the resulting shared secret to be a specific value X. Can Bob choose his Diffie-Hellman value so that, following the protocol, Alice will compute the shared secret X? If so, provide precise details and if not, why not?

A: Bob wants to solve for b in the equation $(g^a)^b \mod p = X$, but this require Bob to solve the discrete log problem, where the base is $g^a \mod p$.

9. (15 points) Suppose that Bob's knapsack private key consists of (3, 5, 10, 23) along with the multiplier $m^{-1} = 6$ and modulus n = 47.

a) Find the plaintext given the ciphertext C = 29. Give your answer in binary.
b) Given m=8, find the public key.

A:
a) First, compute $m^{-1}C = 6 * 29 = 174 = 33 \mod 47$.
Using the superincreasing knapsack in the private key, we find that the plaintext is 0011.
b) Since $m^{-1} * m = 6m = 1 \mod 47$, m = 8.
Multiply each element in the superincreasing knapsack by m and reduce mod 47 to obtain the "general" knapsack, (24, 40, 33, 43).

10. (5 points) Consider the elliptic curve

$$E : y^2 = x^3 + 11x + 19(mod 167)$$

Verify that the point P = (2,7) is on E

A: We have $7^2 = 2^3 + 11 * 2 + 19 \mod 167$, since $49 = 49$, regardless of the modulus.

11. (10 points) Consider a "2 out of 3" secret sharing scheme. Suppose that Alice's share of the secret is (4, 10/3), Bob's share is (6, 2), and Charlie's share is (5, 8/3). What is the secret S? What is the equation of the line?

A: The secret is S = 6 and the line is $2x + 3y = 18$

Submission instructions

- Type your answers using whatever text editor you like, remember to include the index number of each question.
- Export the file to PDF format.
- Name the PDF file based on your BU email ID. For example, if your BU email is "abc@binghamton.edu", then the PDF file should be named as "hw1_abc.pdf".
- Submit the PDF file to Brightspace before the deadline.