CS5285: Information Security for eCommerce Autumn, 2024
Problem Set 1 (Due Date: October 15)

Questions:

1. **Security Services and Mechanisms (10)**:Find a news article about any security-related incident that has been reported in the press since the start of August 2024 (e.g. large hack, data breach, malware, etc.). The even could have taken place before August 2024, but it must have been first reported afterwards. Write a short essay (maximum 400 words) explaining in your own words what has happened. You must mention the type of attackers involved, what the main security services are that were compromised, and what services and mechanisms you think could have been used to mitigate this event. Provide one link to the incident article you are discussing.

2. **Modes of Operation and 'shift cipher' (5-5-5-5-5)**: Suppose that we use a shift cipher that has a 4-bit input and 4-bit output as a block cipher. Let the shift cipher key be $k = 3$, i.e. $E_k(A(0000)) = D(0011)$ and the plaintext be $P =$ BOBALICE (P_0 is B). The conversion between the letters and binary strings are given in the table below. Note that this alphabet only has 16 letters as shown, e.g. $E_k(O) = B$.

A	B	C	D	E	F	G	H
0000	0001	0010	0011	0100	0101	0110	0111
I	J	K	L	M	N	O	P
1000	1001	1010	1011	1100	1101	1110	1111

   (a) Encrypt the plaintext P using CBC mode with $IV = 0011$.

   (b) Encrypt the plaintext P using CBC mode with $IV = 1010$. How does your ciphertext compare to that in 2(a).

   (c) Encrypt the plaintext P using CTR mode with P_0 being encrypted with counter starting at 0 (you can use online/calculator to do decimal to binary conversion, e.g. 1 is 0001, 2 is 0010).

   (d) Use your answer from 2(a). If the MSB bit of C_3 becomes an error, what is the recovered plaintext?

   (e) Use your answer from 2(a). If the block C_3 is lost (receiver does not realise it is missing and process C_4 as C_3), what is the recovered plaintext?

3. **Number Theory (5-5-5-5-5-5 points)**: Show your steps in the following calculations (you can use a calculator but you need to show how you approached to problem - you cannot give me only the answer). Let X be your 8-digit student ID (e.g. 12345678) and Y be the least significant 4-digits of your student ID (e.g. 5678), and consider X and Y to be an integer. **You must use your student ID, other values will be marked incorrect.**

   (a) Compute 41^Y mod 18865 using the square-and-multiply method.

   (b) Calculate $\phi(Y)$.

   (c) gcd(X, 928374827).

   (d) Find integers x and z such that $x \cdot X + z \cdot 928374827 = \gcd(X, 928374827)$.

   (e) Compute 108809^{-1} mod 291452.

   (f) Choose any prime number Z that is smaller than X. Calculate X^X mod Z.

4. **El-Gamal (2-3-3-2)** Consider the El-Gamal encryption scheme and let $p = 13$ and $g = 3$

   (a) Suppose the private key is $x = 5$. Compute the public key y.

   (b) Encrypt the message $M = 6$ using the public key above and $r = 7$.

   (c) Verify your calculation in part (b) above by decrypting the ciphertect you obtained in part (b)

   (d) What security services can you provide using the El-Gamal algorithm shown in the class notes?

5. **Diffie-Hellman(2-2-2-6)** Consider a Diffie-Hellman key exchange with $p = 13$ and $g = 7$.

   (a) Alice picks $x = 5$, what is the public key A will send to Bob?

   (b) Bob picks $y = 11$, what is the public B he will send to Alice?

   (c) What is the shared key K resulting from the exchange?

   (d) One weakness of DH is that it is vulnerable to Man-in-the-Middle attack. How could you modify the exchanged messages in DH to prevent this attack? Clearly state all your assumptions (including any additional cryptographic algorithm or material needed) and the notation you used.

6. **HMAC (10)**

   (a) You are the owner of an online software vendor. Your clients purchase and download programs from you over the Internet. To prevent attackers from adding malware at the end of you programs you decide to use an HMAC to provide data origin authentication. Your chief programmer tells you that they will implement the HMAC as follows:
   HMAC $=h(K||data)$
   Explain why this is not a secure HMAC implementation. How would you suggest they implement an HMAC?