PS1 Solution

Gerhard Hancke

The City University of Hong Kong

October 15, 2024

Q1: Security Services and Mechanisms (10 points) I

Question: 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.

Q1: Security Services and Mechanisms (10 points) II

Solution:

(a) Individual per student, you can find interesting stories anywhere - for example, SANS Newsbytes.

(b) Story must have been published after August 2024, valid link must be provided. [1]

(c) There must be a valid, technically correct summary of the event (not copy-paste from article). [1]

(d) Must mention the type of attacker casual, insiders, criminal, advanced (e.g. state sponsored, hacktivists). [2]

(e) Must correctly use the terminology of service and mechanisms, e.g. confidentiality services and encryption mechanism. If this is not correct, e.g. 'In this case we have a problem with encryption' then 3 marks not awarded. [3]

Q1: Security Services and Mechanisms (10 points) III

- (f) Must identify valid mechanisms to provide the service stated (e.g. if problem was confidentiality, cannot say digital signature). Actual service stated to be compromised not that important unless completely wrong (e.g. data leak listed as integrity problem). [3]

Q1: Security Services and Mechanisms (10 points) IV

Many places to get stories:
Private cybersecurity news aggregation
Example 1: https://www.sans.org/newsletters/newsbites/
Governments
Example 2:
https://www.ncsc.gov.uk/section/keep-up-to-date/threat-reports

Q2: Modes of Operation and 'shift cipher' (5-5-5-5 points) I

Question: Suppose that we use a shift cipher that has a 4-bit input and 4-bit output as a block cipher. Let the key be $k = 3$ and the plaintext be $P =$ BOBALICE. The conversion between the letters and binary strings are given in the table below. Note that this alphabet only has 16 letters, e.g. $E_k(O) = B$ for $k = 3$.

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).

Q2: Modes of Operation and 'shift cipher' (5-5-5-5 points) II

(c) Encrypt the plaintext P using CTR mode with P0 being encrypted with counter starting at 0 (you can use online/calculator to do decimal to binary conversion, e.g.0 is 0000, 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 processes C_4 as C_3), what is the recovered plaintext?

Q2: Modes of Operation and 'shift cipher' (5-5-5-5 points) III

Solution: $P = \text{BOBALICE} = 0001\ 1110\ 0001\ 0000\ 1011\ 1000\ 0010\ 0100$, which consists of 8 blocks of size 4. Since $k = 3$, the encryption of a letter X, say $E_k(A)$, is the letter shifted by 3 from $A >> D$.

Q2: Modes of Operation and 'shift cipher' (5-5-5-5 points) IV

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

$$
\begin{aligned}
C_0 &= E_k(IV \oplus P_0) = E_k(0011 \oplus 0001) = E_k(0010) = E_k(\mathrm{C}) = \mathrm{F} \\
C_1 &= E_k(C_0 \oplus P_1) = E_k(0101 \oplus 1110) = E_k(1011) = E_k(\mathrm{L}) = \mathrm{O} \\
C_2 &= E_k(C_1 \oplus P_2) = E_k(1110 \oplus 0001) = E_k(1111) = E_k(\mathrm{P}) = \mathrm{C} \\
C_3 &= E_k(C_2 \oplus P_3) = E_k(0010 \oplus 0000) = E_k(0010) = E_k(\mathrm{C}) = \mathrm{F} \\
C_4 &= E_k(C_3 \oplus P_4) = E_k(0101 \oplus 1011) = E_k(1110) = E_k(\mathrm{O}) = \mathrm{B} \\
C_5 &= E_k(C_4 \oplus P_5) = E_k(0001 \oplus 1000) = E_k(1001) = E_k(\mathrm{J}) = \mathrm{M} \\
C_6 &= E_k(C_5 \oplus P_6) = E_k(1100 \oplus 0010) = E_k(1110) = E_k(0) = \mathrm{B} \\
C_7 &= E_k(C_6 \oplus P_7) = E_k(0001 \oplus 0100) = E_k(0101) = E_k(\mathrm{F}) = \mathrm{I}
\end{aligned}
$$

Therefore, the ciphertext is FOCFBMBI.

Q2: Modes of Operation and 'shift cipher' (5-5-5-5 points) V

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

$$C_0 = E_k(IV \oplus P_0) = E_k(1010 \oplus 0001) = E_k(1011) = E_k(\mathrm{L}) = \mathrm{O}$$
$$C_1 = E_k(C_0 \oplus P_1) = E_k(1110 \oplus 1110) = E_k(0000) = E_k(\mathrm{A}) = \mathrm{D}$$
$$C_2 = E_k(C_1 \oplus P_2) = E_k(0011 \oplus 0001) = E_k(0010) = E_k(\mathrm{C}) = \mathrm{F}$$
$$C_3 = E_k(C_2 \oplus P_3) = E_k(0101 \oplus 0000) = E_k(0101) = E_k(\mathrm{F}) = \mathrm{I}$$
$$C_4 = E_k(C_3 \oplus P_4) = E_k(1000 \oplus 1011) = E_k(0011) = E_k(\mathrm{D}) = \mathrm{G}$$
$$C_5 = E_k(C_4 \oplus P_5) = E_k(0110 \oplus 1000) = E_k(1110) = E_k(\mathrm{O}) = \mathrm{B}$$
$$C_6 = E_k(C_5 \oplus P_6) = E_k(0001 \oplus 0010) = E_k(0011) = E_k(\mathrm{D}) = \mathrm{G}$$
$$C_7 = E_k(C_6 \oplus P_7) = E_k(0110 \oplus 0100) = E_k(0010) = E_k(\mathrm{C}) = \mathrm{F}$$

Therefore, the ciphertext is ODFIGBGF. The ciphertext results are different.

Q2: Modes of Operation and 'shift cipher' (5-5-5-5 points) VI

- Encrypt the plaintext P using CTR mode with P_0 being encrypted with counter starting at 0:

$$C_0 = E_k(0000) \oplus P_0 = E_k(\mathrm{A}) \oplus \mathrm{B} = \mathrm{D}(0011) \oplus \mathrm{B}(0001) = \mathrm{C}(0010)$$
$$C_1 = E_k(0001) \oplus P_1 = E_k(\mathrm{B}) \oplus \mathrm{O} = \mathrm{E}(0100) \oplus \mathrm{O}(1110) = \mathrm{K}(1010)$$
$$C_2 = E_k(0010) \oplus P_2 = E_k(\mathrm{C}) \oplus \mathrm{B} = \mathrm{F}(0101) \oplus \mathrm{B}(0001) = \mathrm{E}(0100)$$
$$C_3 = E_k(0011) \oplus P_3 = E_k(\mathrm{D}) \oplus \mathrm{A} = \mathrm{G}(0110) \oplus \mathrm{A}(0000) = \mathrm{G}(0110)$$
$$C_4 = E_k(0100) \oplus P_4 = E_k(\mathrm{E}) \oplus \mathrm{L} = \mathrm{H}(0111) \oplus \mathrm{L}(1011) = \mathrm{M}(1100)$$
$$C_5 = E_k(0101) \oplus P_5 = E_k(\mathrm{F}) \oplus \mathrm{I} = \mathrm{I}(1000) \oplus \mathrm{I}(1000) = \mathrm{A}(0000)$$
$$C_6 = E_k(0110) \oplus P_6 = E_k(\mathrm{G}) \oplus \mathrm{C} = \mathrm{J}(1001) \oplus \mathrm{C}(0010) = \mathrm{L}(1011)$$
$$C_7 = E_k(0111) \oplus P_7 = E_k(\mathrm{H}) \oplus \mathrm{E} = \mathrm{K}(1010) \oplus \mathrm{E}(0100) = \mathrm{O}(1110)$$

Therefore, the ciphertext is CKEGMALO.

Q2: Modes of Operation and 'shift cipher' (5-5-5-5 points) VII

(d) Use your answer from 2(a). If the MSB bit of C_3 becomes an error, what is the recovered plaintext?
C_3, which is F (0101) becomes N (1101),
$P_3 = C_2 \oplus D_k(N) = C(0010) \oplus K(1010) = I(1000), P4 = C_3 \oplus D_k(B) = N(1101) \oplus O(1110) = D(0011)$. Plaintext is BOBIDICE A (two blocks are incorrect)

Q2: Modes of Operation and 'shift cipher' (5-5-5-5 points) VIII

- 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?
  C_3 is now lost, new $P_3 = C_2 \oplus D_k(C_4)$, so
  $P_3 = C_2 \oplus D_k(B) = C(0010) \oplus O(1110) = M(1100)$, and
  $P_4 = C_4 \oplus D_k(C_5)$, so
  $C_4 \oplus D_k(M) = B(0001) \oplus J(1001) = I(1000)$. Plaintext is BOBMICE (we lost a block, and one block is incorrect)

Q3: Number Theory (5-5-5-5-5-5 points) I

Question: 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 number (e.g. 5678), and consider X and Y to be an integer.

a. Compute $41^Y \bmod 18865$ 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 $96491^{-1} \bmod 291452$.

f. Choose any prime number Z that is smaller than X. Calculate $X^X \bmod Z$.

Q3: Number Theory (5-5-5-5-5-5 points) II

(a) I choose $X = 48861840$ (Different for individual per student). Use 'square and multiply'

$$
\begin{aligned}
&1840 = 2^4 + 2^5 + 2^8 + 2^9 + 2^{10} \\
&41^{2^1} \bmod 18865 = 41^2 \bmod 18865 = 1681 \bmod 18865 \\
&41^{2^2} \bmod 18865 = 1681^2 \bmod 18865 = 14876 \bmod 18865 \\
&41^{2^3} \bmod 18865 = 14876^2 \bmod 18865 = 8926 \bmod 18865 \\
&41^{2^4} \bmod 18865 = 8926^2 \bmod 18865 = 6581 \bmod 18865 \\
&41^{2^5} \bmod 18865 = 6581^2 \bmod 18865 = 14386 \bmod 18865 \\
&41^{2^6} \bmod 18865 = 14386^2 \bmod 18865 = 7946 \bmod 18865 \\
&41^{2^7} \bmod 18865 = 7946^2 \bmod 18865 = 16626 \bmod 18865 \\
&41^{2^8} \bmod 18865 = 16626^2 \bmod 18865 = 13896 \bmod 18865 \\
&41^{2^9} \bmod 18865 = 13896^2 \bmod 18865 = 15541 \bmod 18865 \\
&41^{2^{10}} \bmod 18865 = 15541^2 \bmod 18865 = 12951 \bmod 18865 \\
&41^{1840} \bmod 18865 \\
=&41^{2^4} \times 41^{2^5} \times 41^{2^8} \times 41^{2^9} \times 41^{2^{10}} \bmod 18865 \\
=&6581 \times 14386 \times 13896 \times 15541 \times 12951 \bmod 18865 \\
=&5776 \bmod 18865
\end{aligned}
$$

Q3: Number Theory (5-5-5-5-5-5 points) III

b. Calculate $\phi(Y)$.
$Y = 1840$ (Different for individual per student)
Start with first prime 2. 1840 divisible by $2^4 = 16$, 1840/16=115, $115/5 = 23$, which is a prime.
$1840 = 2^4.5.23$ so $\phi(1840) = \phi(2^4).\phi(5).\phi(23) = 2^3(1).4.22 = 704$

Q3: Number Theory (5-5-5-5-5-5 points) IV

- $\gcd(X, 928374827)$.
  Use the Euclidean algorithm

$$\gcd(48861840, 928374827)$$
$$\gcd(48861840, 928374827 \bmod 48861840 = 48861707)$$
$$928374827 = 18.48861840 + 48861707$$
$$= \gcd(48861840 \bmod 48861707 = 133, 48861707)$$
$$48861840 = 48861707 + 133$$
$$= \gcd(133, 48861707 \bmod 133 = 34); 48861707 = 367381.133 + 34$$
$$= \gcd(133 \bmod 34 = 31, 34); 133 = 3.34 + 31$$
$$= \gcd(31, 34 \bmod 31 = 3); 34 = 31 + 3$$
$$= \gcd(31 \bmod 3 = 1, 3); 31 = 10.3 + 1$$
$$= \gcd(1, 3) = 1; 3 = 3.1 + 0$$

Q3: Number Theory (5-5-5-5-5-5 points) V

d. Find integers x and z such that $x \cdot X + z \cdot 928374827 = \gcd(X, 928374827)$. Use the extended Euclidean algorithm (which you already did half off in 3c)

Q3: Number Theory (5-5-5-5-5-5 points) VI

$$
\begin{aligned}
1 &= 31 - 10 \times 3 \\
&= 31 - 10 \times (34 - 1 \times 31) = -10 \times 34 + 11 \times 31 \\
&= 11 \times (133 - 3 \times 34) - 10 \times 34 = 11 \times 133 - 43 \times 34 \\
&= 11 \times 133 - 43 \times (48861707 - 133 \times 367381) \\
&= -43 \times 48861707 + 15797394 \times 133 \\
&= 15797394 \times (48861840 - 1 \times 48861707) - 43 \times 48861707 \\
&= 15797394 \times 48861840 - 15797437 \times 48861707 \\
&= 15797394 \times 48861840 - 15797437 \times (928374827 - 18 \times 48861840) \\
&= 15797394 \times 48861840 - 15797437 \times 928374827 \\
&+ 284353866 \times 48861840 \\
&= 300151260 \times 48861840 - 15797437 \times 928374827
\end{aligned}
$$

Q3: Number Theory (5-5-5-5-5-5 points) VII

- Compute $108809^{-1} \bmod 291452$.
  Use Extended Euclidean algorithm to find the inverse

$$291452 = 2 \times 108809 + 73834$$
$$108809 = 1 \times 73834 + 34975$$
$$73834 = 2 \times 34975 + 3884$$
$$34975 = 9 \times 3884 + 19$$
$$3884 = 204 \times 19 + 8$$
$$19 = 2 \times 8 + 3$$
$$8 = 2 \times 3 + 2$$
$$3 = 1 \times 2 + 1$$

Q3: Number Theory (5-5-5-5-5-5 points) VIII

$$
\begin{aligned}
1 &= 3 - 1 \times 2 \\
&= 3 - 1(8 - 2 \times 3) = 3 \times 3 - 1 \times 8 \\
&= 3 \times (19 - 2 \times 8) - 1 \times 8 = 3 \times 19 - 7 \times 8 \\
&= 3 \times 19 - 7 \times (3884 - 204 \times 19) = 1431 \times 19 - 7 \times 3884 \\
&= 1431 \times (34975 - 9 \times 3884) - 7 \times 3884 = 1431 \times 34975 \times 12886 \times \\
&= 1431 \times 34975 - 12886 \times (73834 - 2 \times 34975) \\
&= 27203 \times 34975 - 12886 \times 73834 \\
&= 27203 \times (108809 - 1 \times 73834) - 12886 \times 73834 \\
&= 27203 \times 108809 - 40089 \times 73834 \\
&= 27203 \times 108809 - 40089 \times (291452 - 2 \times 108809) \\
&= 107381 \times 108809 - 40089 \times 291452
\end{aligned}
$$

$$108809^{-1} \bmod 291452 = 107381 \bmod 291452$$

1

Q3: Number Theory (5-5-5-5-5-5 points) IX

- (f) Choose any prime number Z that is smaller than X. Calculate X^X mod Z.
  $48861840^{48861840}$ mod 48861833 (Use Fermat little theorem and mod prime!)
  $= 48861840^{48861832} \times 48861840^8$ mod 48861833
  $= 1 \times 48861840^8$ mod $48861833 = 5764801$ mod 4886183

Q4: El-Gamal (2-3-3-2) I

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?

Solution:

(a) The public key is computed as $g^x = 3^5 \ mod \ 13 = 9$

(b) An El-Gamal ciphertect is in the form of $C = (A, B)$, where $A = g^r = 3^7 \ mod \ 13 = 3$, $B = M \cdot (g^x)^r = 6 \cdot (9^7) \ mod \ 13 = 2$.

Q4: El-Gamal (2-3-3-2) II

(c) The decryption process is performed as follows.
$K = (A)^x = 3^5 \ mod \ 13 = 9$
$M = B \cdot K^{-1} = 2 \cdot 9^{-1} \ mod \ 13 = 2 \cdot 3 \ mod \ 13 = 6$
Thus, the calculation in part (b) is verified.

(d) This question asks you to consider El-Gamal encryption – it can provide confidentiality. This sub-question essentially asks you whether this algorithm can do anything more than encrypt data. The answer is no. There is a signature scheme based on the discrete logarithm problem but it is not the same algorithm. `https://en.wikipedia.org/wiki/ElGamal_signature_scheme` RSA you can use exactly the same crypto system to both encrypt and sign messages (the equations are the same).

Q5: Diffie-Hellman (2-2-2-6) I

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.

Solution:

a. $A = g^x = 7^5 \ mod \ 13 = 11$

b. $B = g^y = 7^{11} \ mod \ 13 = 2$

c. $K = (g^x)^y = 11^{11} \ mod \ 13 = 6$

Q5: Diffie-Hellman (2-2-2-6) II

- (d) You must add data origin authentication to the messages between Alice and BoB (ENC,MAC,SIGN). The prevents Trudy from sending a different message to Bob (or Alice) and the recipient will only use the value to calculate the key if it knows the other legitimate party sent this number. For example, $MAC_{AB}(g^x modp)$ cannot be changed to $MAC_{AB}(g^t modp)$ as Trudy cannot calculate MAC_{AB}.

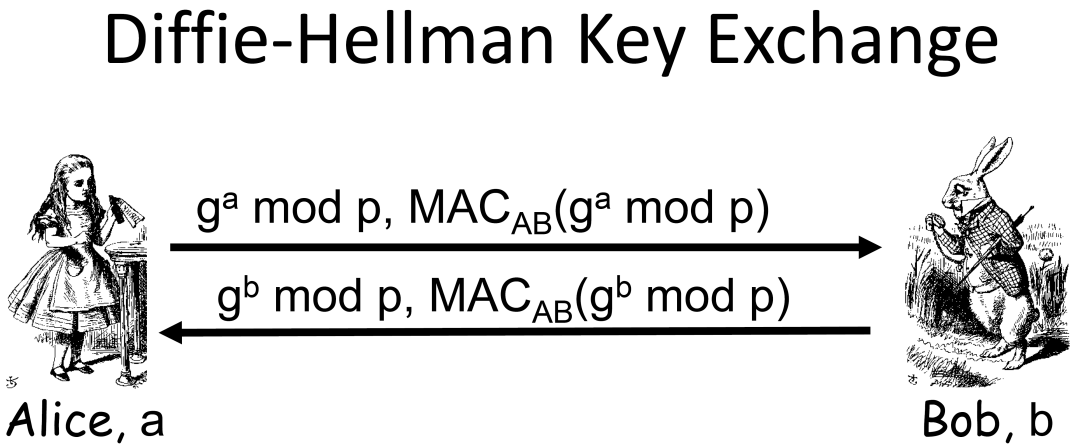

Figure: Example of DH with MAC

Q6: HMAC (10) I

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?

Q6: HMAC (10) II

Solution: An attacker can simple extend the data. Remember that a hash works iteratively - this means if you are hashing $k||data$ you will first hash k, the result is then fed into the next round and hashed with data, repeat until no more data. The final output of the hash is you HMAC but it is also the input to the next block (if you had more data). So an attacker can take this value and extend data and then calculate the updated HMAC (5). It should be $h(k_1||h(k_2, m))$ (5). To get marks you must explain the nature of the attack, the countermeasure and why it prevents the attack.

Q6: HMAC (10) III

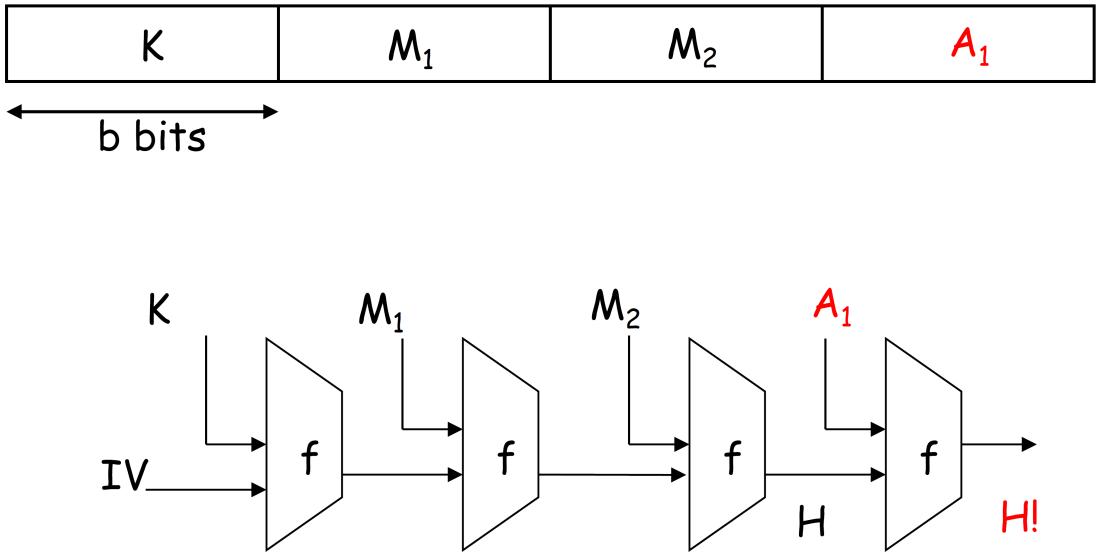

Figure: Extending message