FIT3031
Information & Network Security
Assignment 1 – Summer Semester-B 2017

Submission Guidelines

- **Deadline:** Assignment 1 due on Monday 16th January 2017, 4:00 PM
- **Submission format:** PDF only. You can use any freely available PDF converter to make PDF file from editable one.
- **Submission platform:**
  - Clayton - Softcopy submission on **Moodle**.
- PLEASE INCLUDE **YOUR NAME** AND **SUID** WITHIN THE MAIN PDF SUBMISSION
- Files to submit: ***Assign-1_FirstName_LastName_SUID.pdf***
- **No late submissions ONLY via special consideration request**
- **Late submissions**: An assignment handed in late without prior permission will receive a late penalty of a 5% deduction per day (including Saturday and Sunday) or part thereof, after the due date and time.
- ***Plagiarism****: It is an academic requirement that your submitted work be original. Zero marks will be awarded for the whole submission if there is any evidence of copying, collaboration, pasting from websites, or copying from textbooks. –Plagiarism policy applies to all assessments*

Marks

- *This assignment is worth **20%** of the total unit marks.*
- *The assignment is marked out of **100** nominal marks.*

Assignment Questions

1. **Question-1: [4+4+4+4+4] = 20 marks**

   a. We consider the security services **(A) confidentiality**, **(B) integrity**, **(C) authenticity**, and **(D) non-repudiation**, for a variety of simple protocols. The input is always the plaintext **x**. **y** is the packet sent from Alice to Bob. **Describe which** security **services** are **achieved** by the following protocols.

      1. y = [h(x), x], where h(x) denotes a (collision resistant etc.) hash function. **(4 marks)**

If the packet is **not** exposed to any form of passive or active attack, then this protocol will provide only integrity of the message; Provided the communication is not error prone!

Under real network communications scenario this packet will **not provide any security services to the payload.**

      2. y = [MAC(x), x], where MAC(x) denotes a secure message authentication code such as HMAC. **(4 marks)**

Under real network communications scenario this packet **will provide integrity security services to the payload;** since the HMAC is secure hashed message authenticated code using shared symmetric keys.

      3. y = [encS (h(x)), x], where encS () denotes a secure stream cipher. **(4 marks)**

Under real network communications scenario this packet will **provide integrity security services** to the payload; since the encS (h(x)), is secure stream cipher of the hash of the message using a pseudorandom key stream.

4. y = encB (x, h(x)), where encB () denotes a secure block cipher.

(4 marks)

Under real network communications scenario this packet **will provide confidentiality and integrity, security services** to the payload; since the encB(x, h(x)), is secure block cipher of the hash of the message along with the message using one of the block cipher scheme. E.g. ECB etc...

5. y = encS (x, sig(xm)), where xm is the last block of a long message x; encS () denotes a secure stream cipher and sig(xm) is the signature of message x.

(4 marks)

Under real network communications scenario this packet **will provide confidentiality, integrity, authenticity, and source non-repudiation security services** to the payload; since the encB(x, h(x)), is secure block cipher of the hash of the message along with the message using one of the block cipher scheme. E.g. ECB etc...

2. **Question-2:[6 + (3+5)] =14 marks**

a. With respect to **symmetric key encryption**, explain the problems with key management and its effects. **[6 marks]**

Answer:

The primary weakness of symmetric encryption algorithms is keeping the single key secure. Known as key management, it poses a number of significant challenges.

- The number of keys needs to be managed increase hugely as the user numbers increase; this is given by the formula as (n* (n-1))/ 2. Where n is the number of users.
- KDC needs to be established for appropriate generation and secure and authenticated distribution of these keys.
- Management of short time session keys and long-time master keys require appropriate controls to keep these keys secure; each requiring different handling procedures.
- If a user wants to send an encrypted message to another using symmetric encryption, he must be sure that she has the key to decrypt the message.
- How should the first user get the key to the second user? He would not want to send it electronically through the Internet, because that would make it vulnerable to eavesdroppers. Nor can he encrypt the key and send it, because the recipient would need some way to decrypt the key.

- And if he can even get the get securely to the user, how can be he certain that an attacker has not seen the key on that person's computer?

Key management is a significant impediment to using symmetric encryption. Key management procedures should be in place to support the use of cryptographic techniques and to ensure that only authorized personnel may gain access to sensitive information. Anyone using and implementing their own solutions involving symmetric cryptographic controls advice should be sought on policy and key management, to ensure that data are appropriately secured and that all legal and regulatory requirements have been considered.

(Marks will be allocated based on students focusing on these important symmetric management issues).

b. In the Figure 2.10 ECB (Electronic Code Book) mode, if there is an error in a block of the transmitted ciphertext, only the corresponding plaintext block is affected. However, in the CBC (Cipher Block Chaining) mode, this error propagates. For example, an error in the transmitted **C_2** obviously corrupts **P_2** and **P_3**. This is illustrated in the figure.

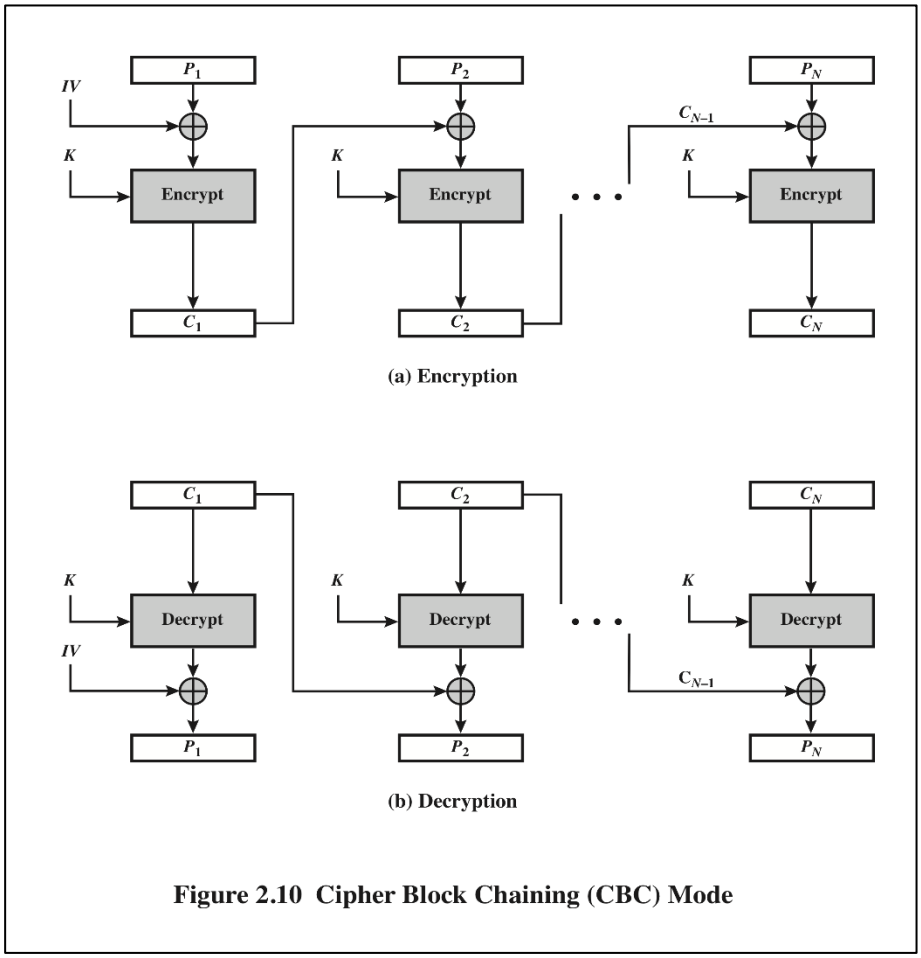

Figure 2.10 Cipher Block Chaining (CBC) Mode

i) Referring to Figure above; Are any blocks beyond **P_3** affected?

[3 marks]

Answer:

No!

For example, suppose C2 is corrupted. The output block P3 depends only on the input blocks C3 and C4

ii) Referring to Figure 2.1 above; suppose that there is a bit error in the source block of P_1. Through how many cipher text blocks is this error propagated? What is the effect at the receiver? **[5 marks]**

Answer:

An error in P1 affects C1. But since C1 is input to the calculation of C2, C2 is affected. This effect carries through indefinitely, so that all cipher-text blocks are affected. (1.5 marks)

However, at the receiving end, the decryption algorithm restores the correct plaintext for blocks except the one in error. You can show this by writing out the equations for the decryption. Therefore, the error only Effects the corresponding decrypted plaintext block. (1.5 marks)

3. **Question-3: [3+3+3 = 9 Marks]**
   Assuming you can do $\mathbf{2^{20}}$ encryptions per second and **key size is 40 bits**:
   a. How long would a brute force attack take? (Both maximum and average values)
   b. Give a scenario where this would be practical and another where it wouldn't.
   c. What happens if you double the key size?

Show the working process of your work in few steps.

Question 3-Ans:

I. Key Size = 40 bit →key space = 2^{40}
Total time = 2^{40} (1 key scheduling + 1 encryption) ÷ (2^{20} encryptions per sec)
Since key scheduling time is not given, we assume the key space has been pre-generated.
Thus,
Maximum time (worst case):
2^{40} encryptions ÷ 2^{20} encryptions per sec
= $2^{(40 - 20)}$ = 2^{20} seconds
≈ 12.14 days
Average time:
= $2^{(40 - 20)}$ ÷ 2 = 2^{19} seconds

≈ 6.06 days
[3 marks]

II. If the time taken to crack the key is shorter than the useful life of the information, or the benefit gained from cracking the key is greater than the effort and resource required to crack it (E.g. fast computer, small key space), brute-force attack is feasible.
[1.5 marks]

Under two circumstances brute-force attack is infeasible:
1. The effort and resource required to crack the key is greater than the benefit gained from cracking the key
2. The time taken to crack the key is longer than the useful life of the information
[1.5 marks]

III. In terms of exhaustively searching the entire key space, if the key size is doubled:
40-bit × 2 = 80-bit key →key space = 2^{80}
Total time = 2^{80} encryptions ÷ 2^{20} encryptions per sec
= $2^{(80 - 20)}$ = 2^{60} seconds
≈ 36558901084.69200202942668696093 4years
Which is $2^{(60 - 20)}$ = 2^{40} times of the time required to exhaustively search a 40-bit key space
[2 marks]

4. Question-4: [3+3+3 = 9 Marks]

User **A** and **B** use Diffie-Hellman algorithm to exchange a shared key and generate public keys of their own. Consider a common prime number ***q=71 and α (a primitive root of q) = 7***. Determine the followings:

a. If user **A** has private key=5, what is **A's** public key?
b. If user **B** has private key=12, what is **B's** public key?
c. What is the shared key?

Show the working process of your work in at least three steps. Consult lecture notes and the text book.

Question 4-Ans

A. $X_A = 5$
$Y_A = a^{XA} \bmod q = 7^5 \bmod 71 = 51$
[3 marks]

B. $X_B = 12$
$Y_B = a^{XB} \bmod q = 7^{12} \bmod 71 = 4$
[3 marks]

C. $Y_B^{XA} \bmod p = 4^5 \bmod 71 = 30$
$Y_A^{XB} \bmod p = 51^{12} \bmod 71 = 30$
[3 marks]

Students should show their working towards the answer:
1 marks for correct formula,
1 mark for showing the calculations,
1 mark for correct result

5. Question-5: [5+5+5 = 15 Marks]

Alice and Bob agree to communicate privately via email using a scheme based on RC4, but they want to avoid using a new secret key for each transmission. Alice and Bob privately agree on a 128-bit key ***k***. To encrypt a message ***m*** consisting of a string of bits, the following procedure is used:

a. Choose a random 80-bit value ***v***
b. Generate the ciphertext $c = RC4(v \| k) \oplus m$
c. Send the bit string $(v \| c)$

Answer the following:

a. Suppose Alice uses this procedure to send a message to Bob. Describe how Bob can recover the message ***m*** from $(v \| c)$ using **k**.
b. b. If an adversary observes several values of $(v_1 \| c_1), (v_2 \| c_2)$ ……. Transmitted between Alice and Bob, how can he/she determine when the same key stream has been used to encrypt two messages?
c. If Alice and Bob agree to use 16-bit Cipher Feedback (CFB) mode instead of RC4, and a bit error occurs in the transmission of a ciphertext; how far does the error propagate?

[5+5+5 = 15 Marks]

Question 5-Ans

A. Since Bob already has the shared key k, after receiving Alice's message(v || c), Bob can extract v from (v || c) and compute:
RC4(v || k) ⊕ c
= RC4(v || k) ⊕ (RC4(v || k) ⊕ m)
= RC4(v || k) ⊕ RC4(v || k) ⊕ m
= 0 ⊕ m
= m
[5 mark]

B. Since k is constant, it's only the vector v that makes the key stream RC4(v || k) different. Therefore, if we observe two message M_1 and M_2 such that
$M_1 = (v_1 \| c_1)$ and $M_2 = (v_1 \| c_2)$,
since the same vertex v_1 appears in both M_1 and M_2, the key stream used to compute c_1 and c_2 must only be $RC4(v_1 \| k)$. Therefore, we can deduce that the same key stream is

used to encrypt two messages.
[5 marks]

C. Block size *b* is 16-bit
AES block size is 128-bit, so shift register size *s* should be the same
For CFB, if one block of transmitted ciphertext is corrupted, *(1 + b/s)* blocks of plaintext blocks will be corrupted, in which the first block is directly affected after the XOR operation, then the error propagates *(b/s)* blocks because the shift register contains the corrupted cipher text block for *(b/s)* shifts.

Therefore, the error propagates (128 / 16) = 8 blocks after the first corrupted block
(Students may write 9 blocks in total as answer, which is also acceptable)
[5 marks]

6. Question-6: [2+2 = 4 Marks]

a. Is it possible to perform encryption operations in parallel on multiple blocks of plaintext in CBC mode? **Justify your answer.**
b. How about decryption? **Justify your answer.** **[3+3 = 6 Marks]**

Question 6-Ans

- In CBC encryption, the input block to each forward cipher operation (except the first) depends on the result of the previous forward cipher operation, so the forward cipher operations cannot be performed in parallel.
- In CBC decryption, however, the input blocks for the inverse cipher function (i.e., the ciphertext blocks) are immediately available, so that multiple inverse cipher operations can be performed in parallel.
- The students have to give some reason and not a simple yes/no answer to get full marks, otherwise deduct 0.5 mark for each part.

7. Question-7: [4+4+4 = 12 Marks]

Consider **p=17** and **q=31** in the RSA encryption/decryption algorithm to be used to encrypt a message **M=15**. Using the algorithm, determine the followings:

a. Generate a public-private key pair.
b. Using the generated public key, encrypt the message to get the cipher text **C**.
c. Apply the private key on C to decrypt the original message **M**.

Show the working process of your work in at least three steps in both encryption and decryption. **[4+4+4 = 12 Marks]**

Question 7-Ans

- Select two prime numbers, in this case p=17, q=31
  Calculate n = pq = 17*31 = 527
  Calculate Euler Totient:
  phi(n) = (p-1)(q-1)
  = (17-1)(31-1) = 480
  Select e such that e is relatively prime to phi(n) = 480,

  GCD(phi(n),e) = 1 (1)
  1<e<Euler_tolerant(n) (2)

  The e = 7 is selected because GCD(480,7) = 1

  Determine d such that de mod 480 = 1 and d < 480
  (d*7) mod 480 = 1

  attempting with different values of we get
  343*7 mod 480 = 2401 mod 480 = 1
  therefore d = 343

  So, public key KU = {e,n}={7,527}
  and private key KR = {d,n}={343,527}
  The students have to show at least few steps of calculations to get full marks, otherwise deduct 1 mark.

- C = M^7(mod 527)

  C = 15^7(mod 527)
  C = 178

  Exploiting the properties of modular arithmetic we get

  15^7(mod 527) = [(15^1mod 527)*(15^2mod 527)*(15^4mod 527)]

  (15^1mod 527) = 15
  (15^2mod 527) = 225
  (15^4mod 527) = 33

  So 15^7(mod 527) = (15*225*33)mod 527 = 380070 mod 527 = 178 therefore encrypted message is 178
  The students have to show at least few steps of calculations to get full marks, otherwise deduct 0.5 mark.
- C = 178

M = C^d mod n
M = 178 ^ 343 mod 527

Exploiting the properties of modular arithmetic we get

178^343(mod 527) = [(178^mod 527)*(178^2mod 527)*(178^4mod 527)*(178^16mod 527)*(178^64mod 527)*(178^256mod 527)] mod 527

As, (178^1mod 527) = 178
(178^2mod 527) = 64
(178^4mod 527) = 407
(178^16mod 527) = (407*407*407*407) mod 527=256
(178^64mod 527) = (256*256*256*256) mod 527 =35
(178^256mod 527) = (35*35*35*35) mod 527=256

So M= (178*64*407*256*35*256) mod 527
= [(178*64*407) mod 527 *(256*35*256) mod 527] mod 527
= [525 *256] mod 527
= 15

The students have to show at least few steps of calculations to get full marks, otherwise deduct

8. Question-8: [3+3+3 = 9 Marks]

In this problem we shall compare the security services that are provided by digital signatures (DS) and message authentication codes (MAC). We assume that Oscar is able to observe all messages sent from Alice to Bob and vice versa. Oscar has no knowledge of any keys but the public one in case of DS. State whether and how DS and MAC protect against each attack. The value ***auth (x)*** is computed with a DS or a MAC algorithm, respectively.

a. (Message Integrity) Alice sends a message ***x = "Transfer $1000 to Mark"***in the clear and also sends ***auth (x)*** to Bob. Oscar intercepts the message and replaces ***"Mark"*** with ***"Oscar".*** Will Bob detect this?
b. (Replay) Alice sends a message ***x = "Transfer $1000 to Oscar"*** in the clear and also sends ***auth (x)*** to Bob. Oscar observes the message and signature and sends them 100 times to Bob. Will Bob detect this?
c. (Authentication with Bob cheating) Bob claims that he received a message x with a valid signature ***auth (x)*** from Alice (e.g., ***"Transfer $1000 from Alice to Bob"***) but Alice claims she has never sent it. Can Alice clear this question **in either case?**

[3+3+3 = 9 Marks]

Question 8-Ans

a. Will be detected with both (i) Ds and (ii) MAC
b. Won't be detected by either DS or MAC. Unless the message includes timestamps. (Hint is use Timestamps if you want to detect it!)

c. (i) DS: Alice e has to force Bob to prove his claim by sending her a copy of the message in question with the signature that was sent earlier. Then Alice can show that message and signature can be verified with Bob's public key. Bob must have generated the message.

9. Question-9: [3+3 = 6 Marks]

For two large prime numbers:

p=671998030559713968361666935769 and **q**=282174488599599500573849980909 in RSA public key cryptosystem if the value of **e** is chosen as **65537**

a. what is the value of the private key **d**? Show the details of your work?
b. If the cipher text **C** is…

C = 4944249168903008379276193468707653713028699999226805308626 3 what is the value of the plaintext **M**?

Hint: *These are calculated using the WolframAlpha web site (www.wolframalpha.com) and no programming is required!*

[3+3 = 6 Marks]

Question 9-Ans

Answer:

Clue: These are calculated using the WolframAlpha web site (www.wolframalpha.com) and no programming is required.

first they need to generate n which is just copying and pasting those numbers with * in between

n = 189620700613125325959116839007395234454467716598457179234021

Then calculating phi n which is just as simple

phi(671998030559713968361666935768*282174488599599500573849980908)=189620700613125325959116839006441061935308403129521662317344

then using the web site and entering:

"multiplicative inverse of 65537 mod 189620700613125325959116839006441061935308403129521662317344"

in the provided space gives the value of d

e=65537

d=1113935177625665662057463463653810959383153565235910096467 3

given the following value of M

M =278623657709

they need to enter:

"278623657709^65537 mod 189620700613125325959116839007395234454467716598457179234021"

which results as follows

C = M^e mod n = 4944249168903008379276193468707653713028699999226805308626 3

then to get back the original message they need to type:

"4944249168903008379276193468707653713028699999226805308626 3^11139351776256656620574634636538109593831535652359100964673 mod 189620700613125325959116839007395234454467716598457179234021"

which would result as follows

M?= C^d mod n = 278623657709