The University of Melbourne

School of Computing and Information Systems

COMP90043 Cryptograph and Security

Semester 2, 2020, Mid Semester Test

Sample Solutions

Test Duration: 40 minutes Test + 5 minutes Reading + 15 minutes Uploading.

Instructions to Students:

- Total marks for the test is 50 (Worth 10% of the final mark in the subject).
- Note that the total time to read, complete the work, scan and upload your responses to this test is 1 hour. The last 15 minutes is for uploading your work.
- Test will be open on 5.15PM and you must submit by 6.15PM Australian Eastern Standard Time (AEST). A late submission will attract 2.5 marks deduction per minute late.
- The test will have two parts: Part A is a quiz on canvas, Part B is this assignment and will have three questions.
- The test is open book, which means you may only use course materials provided via the LMS or the text book but must not use any other resource including the Internet.
- You also must not contact or communicate with any other person (other than teaching team) or make use of the Internet.
- Solutions must be written on blank A4 page paper with pen and pencil. You must write your solutions to each question on a new sheet of paper by clearly identifying the question number.
- You must not use tablet or any electronic device to generate your solution.
- Scanning instructions are already made available on Canvas in an announcement.

Part B

1. Basic Numbers

(a) [5 Marks] Find $35^{-1} \bmod 96$ using Extended Euclidean algorithm discussed in the subject. Show step-by-step working.

Solution:

$$\begin{aligned} 96 &= 35 \times 2 + 26 \\ 35 &= 26 \times 1 + 9 \\ 26 &= 9 \times 2 + 8 \\ 9 &= 8 \times 1 + 1 \end{aligned}$$

Thus $GCD(96, 35) = 1$ and the inverse exists.

$$\begin{aligned} 1 &= 9 - 8 \times 1 \\ 1 &= 9 - (26 - 9 \times 2) \times 1 = 9 \times 3 - 26 \times 1 \\ 1 &= (35 - 26 \times 1) \times 3 - 26 \times 1 = 35 \times 3 - 26 \times 4 \\ 1 &= 35 \times 3 - (96 - 35 \times 2) \times 4 = 35 \times 11 - 96 \times 4 \end{aligned}$$

Hence we have $35^{-1} \bmod 96 = 11 \bmod 96 = 11$.

(b) [5 Marks] Find the smallest non-negative remainder of $(1271^{36000075}+36)^{28}$ divided by 111. Show your working.
HINT: You may need to use various simplifying ideas discussed in lectures and workshop including Euler's and Fermat's theorems.

Solution:
Since $1271 \bmod 111 = 50$, we can first simplify the formula to $(50^{36000075} + 36)^{28} \bmod 111$.
As $111 = 3{*}37$, $\varphi(111) = \varphi(3{\times}37) = \varphi(3){\cdot}\varphi(37) = 2{\times}36 = 72$. By Euler's theorem, we have $50^{72} \bmod 111 = 1$. Hence $50^{36000075} \bmod 111 = 50^{500001\times72+3} = (50^{72})^{500001} \times 50^3 \bmod 111 = 50^3 \bmod 111 = 14$. So we have:

$$\begin{aligned} &(50^{36000075} + 36)^{28} \bmod 111 \\ =&(14 + 36)^{28} \bmod 111 \\ =&50^{28} \bmod 111 \\ =&((50^7)^2)^2 \bmod 111 \\ =&((50^3)^2 \times 50)^2)^2 \bmod 111 \\ =&((14^2 \times 50)^2)^2 \bmod 111 \\ =&(32^2)^2 \bmod 111 \\ =&25^2 \bmod 111 \\ =&70 \end{aligned}$$

2. RSA

(a) [4 Marks] Explain how we may factorise an RSA modulus n if we know a number a such that $a^2 \bmod n = 1$.

Solution:

$$\begin{aligned} a^2 \bmod n &= 1 \\ (a^2 - 1) \bmod n &= 0 \\ (a+1) \cdot (a-1) \bmod n &= 0 \\ (a+1) \cdot (a-1) &= kn \end{aligned}$$

$GCD(a+1, n)$ and $GCD(a-1, n)$ will each give us one factor of n.

(b) [6 Marks] A pair of RSA keys can be generated using two prime numbers p and q, as discussed in the subject. However, in this question you will consider a version of RSA involving three prime numbers p, q and r (such that $n = p \times q \times r$), which follows a similar process to generate a pair of encryption and decryption keys, e and d. Show the equations for generating such a pair of keys for the modified RSA crypto system. Using the parameters $p = 23$, $q = 29$ and $r = 31$, find the minimum possible encryption key e and then compute the corresponding decryption key d. As discussed in the subject, remember to present the keys in the form of $< n, e >$ and $< n, d >$.

Solution:

$$n = p \times q \times r = 23 \times 29 \times 31 = 20677$$

$$\varphi(n) = \varphi(p) \cdot \varphi(q) \cdot \varphi(r) = 22 \times 28 \times 30 = 18480$$

$$e = 13$$

$$d = e^{-1} \bmod \varphi(n) = 13^{-1} \bmod 18480 = 15637$$

Hence public key is $< n = 20677, e = 13 >$,
private key is $< n = 20677, d = 15637 >$.

3. The following equations and figure describe one of the standard modes of usage of symmetric key encryption.

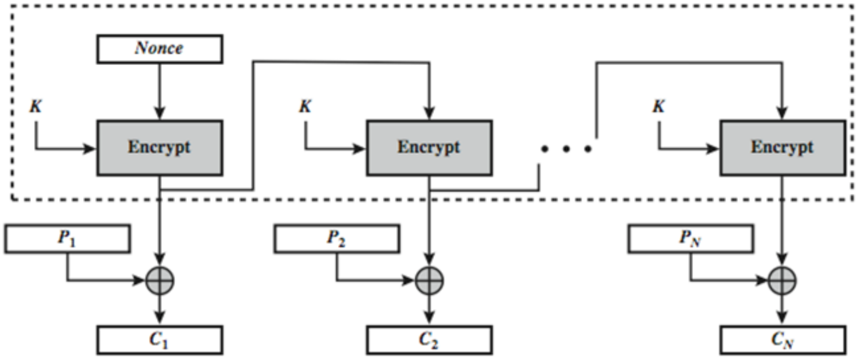

Figure 1: A Standard Mode of Encryption

Encryption: Let IV is the Initial Vector obtained from the Nonce generator.

$$C_1 = P_1 \oplus E_K[IV].$$

$$C_j = P_j \oplus E_K[C_{j-1} \oplus P_{j-1}], j > 1.$$

(a) [2 marks] What is the name of this mode?

Solution:
OFB (output feedback)

(b) [2 Marks] Briefly explain (in no more than two sentences) the purpose of using the **Nonce** in this mode.

Solution:
Nonce can introduce randomness in the encryption process so that outputs from the encryption function can be considered as one-time pad key, which is different in each communication session.

(c) [4 Marks] Using the notations available in the above figure, complete the following decryption functions.

$P_1 =$ .... $P_j =$ ....

Solution:
$P_1 = C_1 \oplus E_k[IV]$
$P_j = C_j \oplus E_k[P_{j-1} \oplus C_{j-1}]$, $j > 1$

(d) [2 Marks] What is the effect on the decrypted plaintext if a one-bit error occurred in the transmission of a ciphertext block C_j? How far does the error propagate?

Solution:
The decrypted plaintext P_j will have one-bit error.
The error does not propagate.