Year and Semester	2018 FALL
Course Number	CS-336
Course Title	Intro. to Information Assurance
Work Number	HA-05
Work Name	Asymmetric Encryption: RSA
Work Version	Version 1
Long Date	Tuesday, 2 October 2018
Author(s) Name(s)	Zane Durkin

Abstract

In this article, since I do not have a partner, I will be completing both sides of the RSA Lab, along with the problems from the textbook and the review questions.

1 RSA Lab

I will be using two prime numbers, p=227 and q=191.
Here are the modulus and Euler totient, Modulus: 43357, Euler Totient:42940
Using these values I can generate a public and private key pair.
For my public key, I will pick a value e such that it has no common factors (except 1) with the Euler totient
My e is: 27
For my private key, I will find a value d such that $d * e$ mod Euler Totient = 1
My private key is: 12723
Since I do not have a partner, I will encrypt a message with my own public key, and then decrypt it with my private key.

1.1 Encryption

My message to encrypt will be HELLOHELLOHELLO
The conversion process is as follows:

Plain Text		Cipher Text	
Trigraph	Trigraph code	Enciphered Code	Quadragraph
HEL	4847	5611	AIHV
LOH	7807	33195	BXCT
ELL	3001	11387	AQVZ
OHE	9650	31569	BUSF
LLO	7736	33322	BXHQ

The cipher text would then be: AIHVBXCTAQVZBUSFBXHQ

1.2 decryption

Now to decrypt the string using my private key. I will be decoding the same string since I do not have a partner to work with.

Cipher Text		Plain Text	
Quadragraph	Quadragraph Code	Deciphered code	Deciphered Trigraph
AIHV	5611	4847	HEL
BXCT	33195	7807	LOH
AQVZ	11387	3001	ELL
BUSF	31569	9650	OHE
BXHQ	33322	7736	LLO

So the deciphered text would be: HELLOHELLOHELLO
which matches the original message.

1.3 RSA Questions

- Private encryption is a one way encryption that prevents third parties from decoding a message after it has been encrypted. The encoded message can only be decoded by the owner of the private key. Symmetric encryption can be encrypted and decrypted using the same key, so either party is able to create and read messages.
- The benefit of private encryption is that the public key does not need to be shared prior to the communication to ensure confidentiality. Symmetric encryption has the benefit of taking much less effort to encrypt and decrypt from a processing standpoint.
- RSA is an acronym of the creators of the algorithm: Ron Rivest, Adi Shamir and Leonard Adelman.
- RSA is very useful for sending encrypted messages across a network with confidentiality ensured.
- Creating a public key requires choosing two prime numbers, and a number that is relatively prime to the phi(n) of the two prime numbers.
- The numbers to be shared are the n value (p*q) and the e value (The number that is relatively prime to n).
- encrypting a message uses the formula $m^e \% n = c$ where m is a message and c is the cipher text Decrypting a message uses a similar formula $c^d \% n = m$.
- RSA by it's self do not make a great use of diffusion, since each bit of the message would normally be encrypted independently, but the use of trigraph codes creates a better use of diffusion since each bit of the message will effect a larger portion of the cipher text.
- RSA provides good use of confusion, since the value of the key effects each bit independently, the key has a dramatic effect on the outputted ciphertext.

2 Problem 21.6 from the textbook [1]

Parts a and c only.

a) $p = 3$
$q = 11$
$e = 7$
$n = 33$
$phi(n) = 20$
$d = 3$
$m = 5$

Encrypting $5^7\%33 = c$
So the Ciphertext would be $c = 14$

Decrypting $14^3\%33 = m$
So the Plaintext would be $m = 5$

c) $p = 7$
$q = 11$
$e = 17$
$n = 77$
$phi(n) = 60$
$d = 53$
$m = 8$

Encrypting $8^{17}\%77 = c$
So the Ciphertext would be $c = 57$

Decrypting $57^{53}\%77 = m$
So the Plaintext would be $m = 8$

3 Review Questions

3.1 Review Question 21.1

hash functions compress data to fit a set size of bits in their output. The compression is done by hashing the data in blocks of a set size.

3.2 Review Question 21.2

SHA requres 5 steps of operations:

- Appending padding buts to the message,
- Appending the original length of the message to the end of the message.
- Initializing the hash buffer with preset values from fractional parts of the first eight prime numbers
- Process message in 1024-bit blocks
- output the final hash of the message

3.3 Review Question 21.3

HMAC is designed to allow for easy replacement of embedded hash functions. The replacement of a hash function is done without any modification to HMAC

3.4 Review Question 21.4

A one-way function is one that is either impossible or really hard to reverse. So finding the original value given the output value would be nearly or entirely impossible.

3.5 Review Question 21.5

Diffie-Hellman's key exchange is done by requiring each party to generate a part of a key, then using two primes and a primitive root to encrypt these keys for transfer across an open network.

References

[1] Stallings, W., and Brown, L. *Computer Security Principles and Practice*, 3 ed. Pearson Education, One Lake Street, Upper Saddle River, New Jersy 07458, 7 2014.