JARAMOGI OGINGA ODINGA UNIVERSITY
OF SCIENCE & TECHNOLOGY
UNIVERSITY EXAMINATIONS 2012/2013
1ST YEAR 2ND SEMESTER EXAMINATION FOR THE DEGREE OF MASTER OF SCIENCE IN INFORMATION TECHNOLOGY

(KISUMU L.CENTRE)

COURSE CODE: IIT 5121

COURSE TITLE: ADVANCED CRYPTOGRAPHY & CYBER SECURITY

DATE: 12/8/2013 **TIME: 9.00-11.00 AM**

DURATION: 3 HOURS

INSTRUCTIONS

1. **This paper consists of 5 Questions.**
2. **Answer Question 1 (Compulsory) and any other 2 questions.**
3. **Write your answers on the answer booklet provided.**

PART A

Q1

1. Today, many Internet businesses and users take advantage of cryptography based on this approach.
   A. public key infrastructure
   B. output feedback
   C. Encrypting File System
   D. single-sign-on

2. Developed by Philip R. Zimmermann, this is the most widely used privacy-ensuring program by individuals and is also used by many corporations.

   A. DSS
   B. OCSP
   C. Secure HTTP
   D. Pretty Good Privacy

3. Which crypto-algorithm offers the best possible mathematical security of any encryption scheme, anywhere and anytime?
   A) RSA
   B) DES
   C) ECC
   D) AES
   E) One-time Pads

4. Network security is a process that is _____.
   A) Abnormal
   B) Examined
   C) Ongoing
   D) Implemented and forgotten

5. This is the encryption algorithm that will begin to supplant the Data Encryption Standard (DES) - and later Triple DES - over the next few years as the new standard encryption algorithm.

   A. Rijndael
   B. Kerberos
   C. Blowfish
   D. IPsec

6. Which of the following reasons would you use to justify the hiring of an outside security assessment firm?

    A) To install anti-virus software
    B) To write a strong security policy
    C) To install the latest service packs and hotfixes
    D) To test your network and devices for vulnerabilities

7. This is the inclusion of a secret message in otherwise unencrypted text or images.

    A. masquerade
    B. steganography
    C. spoof
    D. eye-in-hand system

8. Bob wants to encrypt data and send it to Alice so that only Alice can read the message. Which key should Bob use to encrypt the data?
    A) Alice's public key
    B) Bob's public key
    C) Alice's private key
    D) Bob's private key

9. Which of the following keys are considered stronger, but cryptographically slower, than other types of keys?
    A) Symmetric keys
    B) Secret keys
    C) Delco keys
    D) Asymmetric keys

10. In password protection, this is a random string of data used to modify a password hash.

    A. sheepdip
    B. salt
    C. bypass
    D. dongle

11. Which category of authentication mechanism do tokens employ?
    A) Something you have
    B) Something you know
    C) Something you are
    D) Something you are not

12. S/MIME stands for which of the following?
    A) Secure Mail Internet MAPI Encryption
    B) Snail Mail Inside Multipurpose Encryption
    C) Secure Mail Internet Multipurpose Extension
    D) Secure Multipurpose Internet Mail Extension

13. The function of a hash is to provide _____.
    A) Digital Signatures
    B) Confidentiality
    C) Accountability
    D) Integrity

14. Cryptography is used to achieve the following goals (Check all that apply.)
    A) Confidentiality: To help protect a user's identity or data from being read.
    B) Data integrity: To help protect data from being altered.
    C) Authentication: To assure that data originates from a particular party.
    D) Plaintext transmission

15. A Digital Certificate is used to authenticate _____.
    A) the CA
    B) the sender
    C) the data being sent
    D) that the message was not altered

16. Who first invented wheel cipher?
    A. The Greeks
    B. Julius Caesar
    C. Thomas Jefferson
    D. Charles Babbage

17. SSL uses which of the following *encryption* technologies?
    A) Symmetric
    B) Asymmetric
    C) Symmetric and Assymetric
    D) Digital Certificates

18. Which of the following asymmetric encryption algorithms is based on the difficulty of factoring large numbers?

    A. International Data Encryption Algorithm (IDEA)
    B. RSA
    C. Elliptic Curve Cryptosystems (ECCs)
    D. El Gamal

19. HTTPS is _____.
    A) the same as S/HTTP
    B) HTTP that uses SSL/TLS
    C) an IPSec version of HTTP
    D) HTTP that uses SSH (Secure Shell)

20. This is a mode of operation for a block cipher, with the characteristic that each possible block of plaintext has a defined corresponding ciphertext value and vice versa.

    A. footprinting
    B. hash function
    C. watermark
    D. Electronic Code Book

21. Symmetric algorithms can be categorized into either one of stream or _____ algorithms.
    A) Host
    B) Hash
    C) Lock
    D) block

22. The Digital Signature Algorithm (DSA) is a(n) _____ algorithm.
    A) Secret key
    B) Hash key
    C) Asymmetric key
    D) Session key

23. Of the following, which is most true?

    A. RSA gets its strength from the complexity of using discrete logarithms in a finite field
    B. El Gamal gets its strength from the complexity of using discrete logarithms in a finite field
    C. ECC gets its strength from the complexity of factoring the product of two large prime numbers
    D. Diffie-Hellman gets its strength from the complexity of factoring the product of two large prime numbers

24. This is a trial and error method used to decode encrypted data through exhaustive effort rather than employing intellectual strategies.

    A. chaffing and winnowing
    B. cryptanalysis
    C. serendipity
    D. brute force cracking

25. PKI is an acronym for _____.
    A) Private Key Infrastructure
    B) Public KDC Infrastructure
    C) Personal Key Infrastructure
    D) Public Key Infrastructure

26. A Digital Certificate contains which of the following?
    A) a Private key
    B) a Public key
    C) at least two digital signatures
    D) no more than one digital signature

27. Which of the following key management features allows third-party access to keys, or a portion of a key, under extenuating circumstances?

    A) CRL keys
    B) Backup keys
    C) Key escrow
    D) Direct Trust keys

28. What is a mathematical encryption operation that cannot be reversed called?

    A. DES
    B. Transposition
    C. Substitution
    D. One-way hash

29. Electronic signatures can prevent messages from being:

    A. Erased
    B. Forwarded
    C. Disclosed
    D. Repudiated

30. The Diffie-Hellman algorithm is primarily used to provide which of the following?

    A. Key exchange
    B. Integrity
    C. Non-repudiation
    D. Confidentiality

PART B

Q2Mixed Cryptographic Security Questions (20 Marks)

a) What do we get from the following mod operations (Hint: $a = r \bmod n$): **(6 Marks)**

i) $2 \bmod 11$

ii) $8 \bmod 7$

iii) $-2 \bmod 8$

iv) $-21 \bmod 17$

b) The notation Z_n stands for the set of residues. What does that mean? **(1 Mark)**

c) What is Euclid's algorithm for finding the GCD of two numbers? **(1 Mark)**

d) Given Z_8, **(6 Marks)**

a) Write down all its sets of residues:

b)Find the multiplicative inverse of each nonzero element in Z_8

c)Find the a inverse of each nonzero element in Z_8

e) When the set of all integers is divided by a prime, we obtain a set of remainders that has certain very special properties. What is so special about this set? **(3 Marks)**

Find the prime factorization of 1080

Q3

Answer the questions below regarding key generation with Diffie-Hellman and RSA.

a) Cryptographically speaking, what is the main method of building a shared secret over a public medium? **(1 Mark)**

b) What's the difference between Diffie-Hellman and RSA? **(2 Marks)**

c) Suppose the Diffie-Hellman public values *p* and *g*are 7 and 4, respectively. Compute alegal *y* value. **(4 Marks)**

d) Suppose your partner's *y* value is 3. What is your shared key? **(4 Marks)**

e) Suppose that you are computing an RSA key pair. What are *p* and *q* and $\emptyset(n)$ for an$n = 51$? **(4 Marks)**

f) Find a legal RSA public key pair for this *p* and *q*. **(4 Marks)**

g) How many possible values for *e* are there? **(1 Marks)**

Q4

a) What's the difference between symmetric and public-key cryptography **(2 Marks)**

b) What's the main problem with the traditional symmetric-key cryptography is solved by public-key cryptography? **(2 Marks)**

c) Give the steps necessary to create public and private keys in the RSA algorithm for public-key cryptography? **(5 Marks)**

d) RSA Cryptosystems Problem

Given the following parameters:

```
P = 13<-  first prime number (destroy this after computing E and D)
Q = 43    <-  second prime number (destroy this after computing E and D)
T = 21
```

i) Find: N, Ø(N), *e*, and *d*, and ciphertext*C*. **(6 Marks)**

ii) use the exponentiation to decrypt the ciphertext*C* found in part (i). **(5 Marks)**

Q5

a) Why is there all this excitement about Elliptic Curve Cryptography? **(1 Mark)**

b) How do we construct the number system to use for ECC? **(1 Mark)**

c) ECC uses numbers that correspond to points on elliptic curves. What is an elliptic curve? Does it have anything to do with an ellipse? **(1 Mark)**

d) What is the geometrical interpretation of the group law that is used for the numbers drawn from the elliptic curves in ECC? **(1 Mark)**

e) What is the fundamental reason for why ECC can use shorter keys for providing the same level of security as what RSA does with much longer keys? **(1 Mark)**

f) Given the Weierstraβ form of Elliptic curve cryptography: $E/K:\ Y^2 = X^2 + aX + b$
Start the conditions required to use it in ECC. **(3 Marks)**

g) Let the prime number $p = 23$ and consider an elliptic curve $E:\ y^2 = x^3 + x + 3 \bmod 23$ defined over F_{23}. **(9 Marks)**

i) Show that the curve satisfy the condition to be used for constructing Elliptic curve cryptosystems

ii) Determine the quadratic residues Q_{23} from the reduced set of residue $\mathbf{Z}_{23} = \{1, 2, 3, \ldots, 21, 22\}$

iii) For $0 \le x < p$, compute, $y^2 = x^3 + x + 3 \bmod 23$, determine if y^2 is in the set of quadratic residues Q_{23}:

x	0	1	2	3	4	5	6	7	8	9	10	11
y^2												
$y^2 \in Q_{23}$?												
y_1												
y_2												

x	12	13	14	15	16	17	18	19	20	21	22
y^2											
$y^2 \in Q_{23}$?											
y_1											
y_2											

iv) Write all the points in $E(\mathrm{F}_{23})$ **(3 Marks)**

Q6

a) Caser cipher uses which type of algorithm. **(1 Mark)**

b) Write the Caesar shift as a function. (Namely, f(x) = **x+3** %26. Hint: x is the value of the plaintext alphabetic characters.) **(3 Marks)**

c) Using the affine cipher function f(x) = (ax + b)%26, to encrypt the word "ZEBRA" using the affine cipher with the encryption keys **a = 11, b = 8.** **(5 Marks)**

d) What's the difference between encoding, encryption, and hashing? **(3 Marks)**

e) Expand on Claude Shannon's theorem. Differentiate the term confusion and diffusion as envisaged by Shannon to strengthen crypto-algorithm. **(3 Marks)**

f) Use the extended Euclidean algorithm to compute the greatest common divisor d of 654 and 123and to find integers *m* and *n* such that $64m + 123n = d$. **(5 Marks)**