VI Semester B.C.A. Examination, May/June 2018
(CBCS) (F + R)
(2016-17 and Onwards)
COMPUTER SCIENCE
BCA – 603 : Cryptography and Network Security

Time : 3 Hours Max. Marks : 100

Instruction : *Answer **all** the Sections.*

SECTION – A

Answer **any ten** questions. **Each** question carries **two** marks : **(10×2=20)**

1. What is cryptosystem ?
2. Define Hashing.
3. What are the basic properties of divisibility ?
4. Define cipher text with an example.
5. What is Brute Force attack ?
6. Write any two applications of RSA algorithm.
7. Define Encryption and Decryption.
8. What is Trapdoor one-way function ?
9. Explain Avalanche Effect.
10. What is message padding ?
11. Define digital signature.
12. What are the protocols used to provide IP security ?

SECTION – B

Answer **any five** questions. **Each** question carries **five** marks. **(5×5=25)**

13. Discuss the classification of security goals.
14. Find GCD (2740, 1760) using Euclidean Algorithm.

15. Differentiate between block cipher and a stream cipher.

16. Explain caesar cipher with an example.

17. Explain Fermat's little theorem.

18. What is primality test ? Explain in brief.

19. Explain cipher Feedback Mode.

20. Explain the practical applications of watermarking.

SECTION – C

Answer **any three** questions. **Each** carries **fifteen** marks. **(3×15=45)**

21. a) Explain in detail the taxonomy of attacks with relation to security goals. **10**
    b) Discuss Extended Euclidean Algorithm. **5**

22. a) Explain steps in DES Algorithm. **10**
    b) Discuss any two modes of operations in DES. **5**

23. a) State and explain Chinese Remainder Theorem with an example. **10**
    b) Discuss different attacks on RSA. **5**

24. a) Explain digital signature process with its security mechanism. **10**
    b) Write a note on Kerberos. **5**

25. a) Explain Public Key Infrastructure (PKI) in detail. **10**
    b) Differenciate between MIME and S/MIME. **5**

SECTION – D

Answer **any one** question. **Each** question carries **ten** marks. **(1×10=10)**

26. Explain Diffie-Helman key exchange technique with an example. **10**

27. a) Explain SSL Handshake protocol action. **5**
    b) Write a note on PGP services. **5**

VI Semester B.C.A. Examination, May 2017
(CBCS) (2016-17 and Onwards)
COMPUTER SCIENCE
BCA-603 : Cryptography and Network Security

Time : 3 Hours Max. Marks : 100

***Instruction** : Answer **all** the Sections.*

SECTION – A

Answer **any ten** questions. **Each** question carries **two** marks : **(10×2=20)**

1. What is information security ?
2. What is data integrity ?
3. Who is cryptanalyst ?
4. Define symmetric key cryptography.
5. What is FIPS ?
6. What is permutation process in cryptography ?
7. What is co-prime ? Give examples.
8. What is integer factorization ?
9. Define stream cipher.
10. What is payload ?
11. What is a session ?
12. What is IPSec ?

SECTION – B

Answer **any five** questions. **Each** question carries **five** marks : **(5×5=25)**

13. Explain symmetric key encryption model with a neat diagram.
14. Explain various security mechanisms.
15. Explain Euclid's algorithm with example.
16. Explain transpositional Cipher with an example.

P.T.O.

17. Explain CBC mode of operation.
18. Explain digital signature process with a neat diagram.
19. Explain PGP services.
20. Compare SSL and TLS protocols.

SECTION – C

Answer **any three** questions. **Each** carries **fifteen** marks : **(3×15=45)**

21. a) Explain key elements of public key encryption. **8**

    b) Differentiate equality and congruence with examples. **7**

22. a) Draw the block diagram of DES algorithm. Explain briefly. **8**

    b) Write a short note on multiple DES. **7**

23. a) Explain Fermat's theorem of primality test. **7**

    b) Explain RSA algorithm with one example. **8**

24. a) Write a short note on Whirlpool hash function. **7**

    b) Explain Diffie-Helman key agreement. **8**

25. a) Write a short note on IKE. **7**

    b) Explain the modes of IPSec. **8**

SECTION – D

Answer **any one** question. **Each** question carries **ten** marks : **(1×10=10)**

26. Explain one round of processing in AES.

27. Explain SHA-512 algorithm with a neat diagram.