COMP/IT – 424 HOMEWORK ASSIGNMENT 3

TRUE OR FALSE

T F 1. AES uses a Feistel structure.

T F 2. At each horizontal point, **State** is the same for both encryption and decryption.

T F 3. DES is a block cipher intended to replace AES for commercial applications.

T F 4. Virtually all encryption algorithms, both conventional and public-key, involve arithmetic operations on integers.

T F 5. Compared to public-key ciphers such as RSA, the structure of AES and most symmetric ciphers is quite complex and cannot be explained as easily as many other cryptographic algorithms.

T F 6. InvSubBytes is the inverse of ShiftRows.

T F 7. The ordering of bytes within a matrix is by column.

T F 8. In the Advanced Encryption Standard the decryption algorithm is identical to the encryption algorithm.

T F 9. The S-box is designed to be resistant to known cryptanalytic attacks.

T F 10. As with any block cipher, AES can be used to construct a message authentication code, and for this, only decryption is used.

T F 11. The Rijndael developers designed the expansion key algorithm to be resistant to known cryptanalytic attacks.

T F 12. AES can be implemented very efficiently on an 8-bit processor.

T F 13. Plaintext is transformed into ciphertext using two keys and a decryption algorithm.

T F 14. Public-key encryption is more secure from cryptanalysis than

symmetric encryption.

T F 15. Much of the theory of public-key cryptosystems is based on number theory.

T F` 16. If the authenticator is encrypted with the sender's private key, it serves as a signature that verifies origin, content, and sequencing.

T F 17. A trap-door one-way function is easy to calculate in one direction and infeasible to calculate in the other direction unless certain additional information is known.

T F 18. A public-key encryption scheme is not vulnerable to a brute-force attack.

MULTIPLE CHOICE

1. The Advanced Encryption Standard was published by the _____ in 2001.

   A. ARK B. FIPS

   C. IEEE D. NIST

2. The AES cipher begins and ends with a(n) _____ stage because any other stage, applied at the beginning or end, is reversible without knowledge of the key and would add no security.

   A. Substitute bytes B. AddRoundKey

   C. MixColumns D. ShiftRows

3. In the AES structure both encryption and decryption ciphers begin with a(n) _____ stage, followed by nine rounds that each include all four stages, followed by a tenth round of three stages.

   A. Substitute bytes B. AddRoundKey

   C. MixColumns D. ShiftRows

4. The final round of both encryption and decryption of the AES structure consists of _____ stages.

A. one B. two

C. four D. three

5. The first row of State is not altered; for the second row a 1-byte circular left shift is performed; for the third row a 2-byte circular left shift is performed; and for the fourth row a 3-byte circular left shift is performed. This transformation is called _____ .

A. AddRoundKey B. ShiftRows

C. MixColumns D. Substitute bytes

6. The _____ is when a small change in plaintext or key produces a large change in the ciphertext.

A. avalanche effect B. Rcon

C. key expansion D. auxiliary exchange

7. The AES encryption round has the structure:

A. ShiftRows, MixColumns, SubBytes, InvMixColumns

B. SubBytes, ShiftRows, MixColumns, AddRoundKey

C. MixColumns, ShiftRows, SubBytes, AddRoundKey

D. InvShiftRows, InvSubBytes, AddRoundKey, InvMixColumns

8. In the general structure of the AES encryption process the input to the encryption and decryption algorithms is a single _____ block.

A. 32-bit B. 256-bit

C. 128-bit D. 64-bit

9. Public-key encryption is also known as _____ .

A. digital-key encryption B. asymmetric encryption

C. one way time exchange encryption D. optimal-key encryption

10. Asymmetric encryption can be used for _____ .

A. both confidentiality and authentication

B. neither confidentiality nor authentication

C. confidentiality

D. authentication

11. Plaintext is recovered from the ciphertext using the paired key and a _____ .

A. digital signature B. recovery encryption

C. decryption algorithm D. encryption algorithm

12. The most widely used public-key cryptosystem is _____ .

A. optimal asymmetric encryption

B. asymmetric encryption

C. RSA

D. DES

13. Public-key algorithms are based on _____ .

A. permutation B. mathematical functions

C. substitution D. symmetry

14. A _____ is a cryptographic algorithm that uses two related keys, a public key and a private key. The two keys have the property that deriving the private key from the public key is computationally infeasible.

    A. Private Key (Symmetric) Cryptographic Algorithm

    B. Key Exchange Cryptographic Algorithm

    C. Public Key (Asymmetric) Cryptographic Algorithm

    D. RSA Digital Cryptographic Algorithm

15. A public-key encryption scheme has _____ ingredients.

    A. six B. four

    C. eight D. two

16. The key used in symmetric encryption is referred to as a _____ key.

    A. public B. secret

    C. private D. decryption

17. Two issues to consider with the computation required to use RSA are encryption/decryption and _____ .

    A. time complexity B. trap-door one-way functions

    C. key generation D. asymmetric encryption padding

18. _____ depend on the running time of the decryption algorithm.

    A. Mathematical attacks B. Timing attacks

    C. Chosen ciphertext attacks D. Brute-force attacks

SHORT ANSWER

1. The _____ is a block cipher intended to replace DES for commercial applications. It uses a 128-bit block size and a key size of 128, 192, or 256 bits.

2. The National Institute of Standards and Technology chose the _____ design as the winning candidate for AES.

3. The AES cipher consists of N rounds, where the number of rounds depends on the _____ .

4. The first N - 1 rounds consist of four distinct transformation functions: SubBytes, ShiftRows, AddRoundKey, and _____ .

5. The forward substitute byte transformation, called _____ , is a simple table lookup.

6. The _____ transformation operates on each column individually. Each byte of a column is mapped into a new value that is a function of all four bytes in that column.

7. The mix column transformation combined with the _____ transformation ensures that after a few rounds all output bits depend on all input bits.

8. The AES key expansion algorithm takes as input a four-word (16-byte) key and produces a linear array of _____ words (176 bytes).

9. _____ affects the sequence of bytes in State but does not alter byte contents and does not depend on byte contents to perform its transformation.
10. _____ encryption is a form of cryptosystem in which encryption and decryption are performed using a public key and a private key.

11. A _____ is when two sides cooperate to exchange a session key.

12. Asymmetric encryption transforms plaintext into _____ using one of two keys and an encryption algorithm.

13. The difficulty of attacking _____ is based on the difficulty of finding the prime factors of a composite number.

14. The ____ is a set of policies, processes, server platforms, software and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates.

15. "The sender 'signs' a message with its private key. Signing is achieved by a cryptographic algorithm applied to the message or to a small block of data that is a function of the message," is a description of a _____ .

16. A _____ is an attack in which the adversary chooses a number of ciphertexts and is then given the corresponding plaintexts, decrypted with the target's private key.

PROBLEMS

1. Perform encryption and decryption using the RSA algorithm for the following:

a. p = 3;q=11;e=7;M=5
b. p=7;q=11;e=17;M=8

2. This problem illustrates a simple application of the CCA attack. Bob intercepts a ciphertext **C** intended for Alice and encrypted with Alice's public key **e**. Bob wants to obtain the original message $\mathbf{M = C^d \bmod n}$. Bob chooses a random value **r** less than **n** and computes:

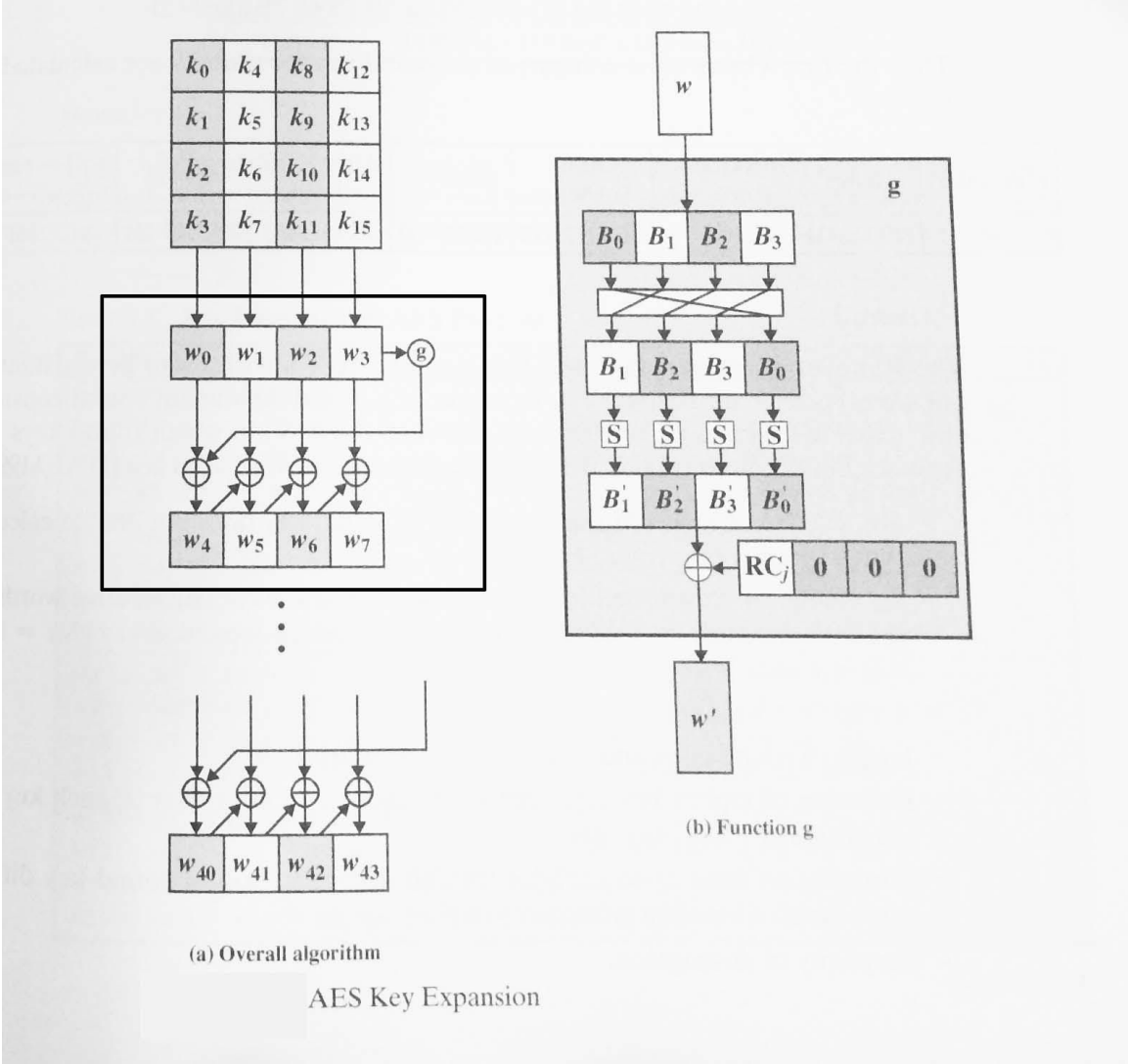
$$\mathbf{Z = r^e \bmod n}$$
$$\mathbf{X = ZC \bmod n}$$
$$\mathbf{t = r^{-1} \bmod n}$$

Nest Bob gets Alice to authenticate (sign) **X** with her private key d thereby decrypting **X.** Alice return $\mathbf{Y = X^d \bmod n}$
Show how Bob can use the information now available to him to determine **M**.

3. Show the first eight words of the key expansion for a 128-bit key of all zeros in an AES encryption scheme.

Use the algorithm as shown in the figure given below where the function g is given as follows

a. a circular one byte circular left shift on the input word.
b. a substitution on each byte of the word using the AES 256 byte S-BOX (this is the same S-box we used in class to find the output of the first round of AES and is posted on CILearn.
c. An EXOR with a Round Constant which for round one is given as (01,00,00,00) hex.



AES Key Expansion