

Name: _____

ID: _____


Question 1: (50 points) [ABET Outcome e]

Circle the *one answer* that best answers the question. Please fill in your multiple choice answers using **CAPITAL** letters!

1	2	3	4	5	6	7	8	9	10	11	12	13

14	15	16	17	18	19	20	21	22	23	24	25

- Eve has bet (راهن) Bob that she can figure out the AES secret key he shares with Alice if he will simply encrypt 20 messages for Eve using that key. For some unknown reason, Bob agrees. Eve gives him 20 messages, which he then encrypts and emails back to Eve. What kind of attack is Eve using here?
 - This is a chosen-plaintext attack
 - This is a ciphertext-only attack
 - This is a chosen-ciphertext attack
 - This is a known-plaintext attack
- The Shannon principle of “diffusion”
 - makes relationship between ciphertext and key as complex as possible
 - diffuses the plaintext among huge subset of plaintexts
 - dissipates statistical structure of plaintext over bulk of ciphertext.
 - diffuses the key and the plaintext among a subset of plaintexts
- To encrypt a series of plaintext blocks P_1, P_2, \dots, P_n using a block cipher E operating in electronic code book (ECB) mode, each ciphertext block C_1, C_2, \dots, C_n is computed as $C_i = E(k, P_i)$. Which of the following is not a property of this block cipher mode?
 - Any repeated plaintext blocks will result in identical corresponding ciphertext blocks.
 - Decryption can be fully parallelized.
 - If a ciphertext block is modified or corrupted, then after decryption the corresponding plaintext block and all the following plaintext blocks will be affected.
 - None of the above; that is, (A), (B), and (C) are all properties of the ECB block cipher mode.
- If by $E_K(\)$ we denote the encryption function of a block cipher with a key K , and if the mode of operation is $C_i = E_K(P_i \oplus C_{i-1})$ then the mode of operation is _____.
 - CFB
 - CBC
 - OFB
 - CTR

5. Why is the Double version of the 56-bit DES much less secure than a single 112-bit DES?
- Because the plaintext is encoded twice, with different keys
 - Because Double DES can be attacked by “meet-in-the-middle”
 - Because Double DES can be attacked by “man-in-the-middle”
 - Because Double DES can be attacked by “brute-force”
6. Let C be a block cipher of block size n . If C is not an arbitrary permutation, but has key length k , how many tries will be required to break C through exhaustive key search?
- 2^n
 - $2^{n/2}$
 - $(2^n)!$
 - 2^k
-  7. Chinese Remainder Theorem is used in RSA in order
- To compute the private exponent d
 - To find strong prime numbers
 - To speed up the decryption with the private key approximately 4 times
 - To speed up the encryption with the public key approximately 4 times
8. If the Miller-Rabin algorithm return the value “composite” then the investigated number is:
- composite with at least 3 factors
 - prime with some positive probability
 - composite with some positive probability less than 1.0
 - definitely composite
9. How many elements are contained in the group of units Z_m^* , if $m = 3 \cdot 13$?
- 39
 - 24
 - 13
 - 3
10. The attack that is exploiting the variations in operations that depend on different 0s and 1s in the private key are called
- timing attack
 - linear attack
 - differential attack
 - exponentiation attack
11. On which claimed unsolved mathematical “hard problem” is Elliptic Curve Cryptography cryptosystem based?
- Discrete logarithm problem
 - Integer factoring problem
 - Elliptic Curve Integer factoring problem
 - Elliptic Curve Discrete Logarithm Problem
12. An ECC (Elliptic Curve Cryptography) scheme with size of 256 bits has an equivalent security of a symmetric scheme with
- 128 bits
 - 256 bits
 - 512 bits
 - 3072 bits

13. Which of the following properties must a cryptographic hash function provide?
- Key revocation.
 - A deterministic mapping from input to output.
 - One-to-one mapping of input to output.
 - Ease of finding an input that matches a given hash.
14. What does it mean that a hash function H is “collision resistant”?
- It is easy to compute $h = H(M)$ for any message M
 - Given h , it is infeasible to find x such that $H(x) = h$
 - Given x , it is infeasible to find y such that $H(y) = H(x)$
 - It is infeasible to find any x, y such that $H(y) = H(x)$
15. If we have a hash function with a digest size of n bits, with the birthday paradox attack approximately how much hash operations we need in order to find a collision
- $2^{n/2}$
 - $2n$
 - 2^n
 - 2^{n-1}
16. If we perform the following operations:
 $Hash[(k^+ \oplus opad || Hash(k^+ \oplus ipad) || M)]$
 where k^+ is a properly padded secret key, $opad$ and $ipad$ are specific padding constants, and M is a message, and $||$ denote the concatenation then we have performed:
- 2-Hash operation
 - CMAC operation
 - HMAC operation
 - Double-Hash operation
17. Message authentication codes (MAC) and digital signatures both serve to authenticate the content of a message. Which of the following best describes how they differ?
- A MAC can be verified based only on the message, but a digital signature can only be verified with the secret key used to sign the message.
 - A MAC can be verified based only on the message, but a digital signature can only be verified with the public key of the party that signed the message.
 - A MAC can only be verified with the secret key used to generate it, but a digital signature can be verified based only on the message.
 - A MAC can only be verified with the secret key used to generate it, but a digital signature can be verified with the public key of the party that signed the message.
18. Let $C(K, M)$ denote a message authentication code function, produced for the message M and a shared key K . Let $E(K, M)$ denote encryption of a message M with a key K , and let $||$ denote the concatenation. If Alice send to Bob the following information: $E(K_2, M) || C(K_1, E(K_2, M))$ where K_1 and K_2 are shared secret keys, then it is
- just a message authentication
 - message authentication and confidentiality where authentication is tied to the plaintext
 - message authentication and confidentiality where authentication is tied to the ciphertext
 - just a message confidentiality
19. Let (PU_A, PR_A) are the public and private key of Alice, and (PU_B, PR_B) are the public and private key of Bob. Let $H()$ be a hash function, $E(\text{Key}, \text{Data})$ denote an encryption, and $D(\text{Key}, \text{Data})$ decryption operation, $||$ denote a concatenation and Doc be a document. The digital signature algorithm performed by Alice, on the document Doc can be described as:
- $\text{Doc} || E(PU_A, H(\text{Doc}))$
 - $\text{Doc} || E(PU_B, H(\text{Doc}))$
 - $\text{Doc} || D(PR_B, H(\text{Doc}))$
 - $\text{Doc} || E(PR_A, H(\text{Doc}))$

20. If an attacker can forge a signature for at least one message, but he/she does not have control over the message, then the attack is characterized as:
- A. Universal forgery
 - B. Selective forgery
 - C. Existential forgery
 - D. Masquerading forgery
21. Which three public-key algorithms can be used for digital signature:
- A. RSA, Elliptic Curve, DSS
 - B. RSA, Elliptic Curve, Diffie-Hellman
 - C. Elliptic Curve, Diffie-Hellman, DSS
 - D. RSA, Diffie-Hellman, DSS
22. In certification authority (CA) hierarchy which action has to be performed when a user's private key is compromised?
- A. Generation of a new private key
 - B. Generation of a new private/public key pair
 - C. Certificate revocation
 - D. Deletion of the user's certificate
23. What is the trusted registry that guarantees the authenticity of client and server public keys?
- A. Public key notary (كاتب العدل).
 - B. Certification authority.
 - C. Key distribution center.
 - D. Key revocation certificate.
24. The key exchange protocol is vulnerable to a _____ attack because it does not authenticate the participants.
- A. chosen ciphertext
 - B. man -in-the-middle
 - C. side channel
 - D. replay
25. Which of the following is a correct URL of a web site using the SSL protocol?
- A. http:// www.google.com
 - B. https:// www.google.com
 - C. https:// www.google.com
 - D. https:// www.google.com

Question 2: (20 points) RSA [ABET Outcome a]

- a) (10 points) Alice uses the RSA signature scheme with primes $p=13$ and $q=23$ and the verification exponent $e=53$. What is Alice's private signing key? Alice signs the digital document $D = 100$. What is the signature?

- b) (5 points) If the ciphertext message produced by RSA encryption with the key $(e, n) = (7, 33)$ is 29, what is the plaintext message?

- c) (5 points) Alice and Bob have the same modulus n for RSA, and encryption exponents e_A and e_B with $\gcd(e_A, e_B)=1$. Charles sends them the same message m encrypted with these keys, resulting in the ciphertexts c_A and c_B . Eve intercepts both c_A and c_B . How can she find m ?

Question 3: (20 points) Diffie-Hellman, Elgamal and ECC [ABET Outcome a]

- a) (5 points) Alice and Bob use the Diffie-Hellman algorithm to exchange a secret key. Eve intercepts the following values: $q = 283$, $g = 12$, $Y_A = 77$, and $Y_B = 196$. Where g is a primitive root of the prime number q . Y_A is Alice's public key and Y_B is Bob's public key. Compute shared secret key (K).

b) (10 points) Alice and Bob use the Elgamal algorithm. Alice chooses a *prime number* $q=107$ and $\alpha = 2$ as primitive root of q . she select her private key $X_A= 67$.

i. What is Alice's public key

ii. Bob wants to encrypt a message $M=66$ and sends it to Alice. He chooses a random integer $k=45$. What is the encrypted message?

iii. Show how Alice decrypts the message received from Bob

c) (5 points) Consider the elliptic curve $E_{23}(1, 1)$. Let $P=(3, 10)$ and $Q=(9,7)$. Find $R = P + Q$.

$$x_R = (\lambda^2 - x_P - x_Q) \bmod q$$

$$y_R = (\lambda(x_P - x_R) - y_P) \bmod q$$

where

$$\lambda = \begin{cases} \left(\frac{y_Q - y_P}{x_Q - x_P} \right) \bmod q & \text{if } P \neq Q \\ \left(\frac{3x_P^2 + a}{2y_P} \right) \bmod q & \text{if } P = Q \end{cases}$$

Question 4: (10 points) [ABET Outcome e] Consider the SSL protocol in Figure 1.

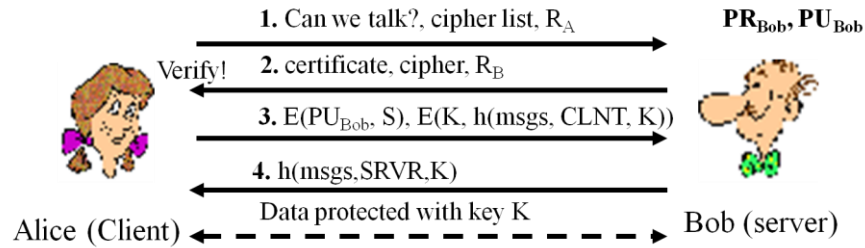


Figure 1: Simplified SSL

- S is known as pre-master secret
- $K = h(S, R_A, R_B)$
- “msgs” means all previous messages
- $CLNT$ and $SRVR$ are constants

a) Suppose that the nonces are R_A and R_B are removed from the protocol and we define $K=h(S)$. What is the effect, if any, does this have on the security of the authentication protocol.



b) Suppose that we change message four to $HMAC(msgs, SRVR, K)$. What effect, if any, does this have on the security of the authentication protocol?



c) Suppose that we change message three to $E(PU_{Bob}, S), h(msgs, CLNT, K)$. What effect, if any, does this have on the security of the authentication protocol?



d) Alice authenticates Bob, not vice-versa. Why would server not authenticate client? How does client authenticate server?

e) Briefly describe an SSL client can check a server’s certificate for validity