,x

1,Underlying framework analysis helps to determine the known vulnerabilities in a particular product being used. [T/F]

2,Cross-site scripting attack seeks to violate which of the following?
a) Password management policy
b) Server configuration policy
c) Minimum access control policy
d) Same origin policy

3,Which of the enumerated form fields cannot possibly be used to insert malicious data? <More than one correct answer may be possible>

A. Any field with style="visibility:hidden"
B. Text Boxes
C. Radio Buttons
D. HTML 5 Radio Buttons
E. Drop Down Lists
F. All of these
G. None of these

4,An HttpOnly cookie can be accessed by client-side JavaScript, true or false?

5,2. Software attestation and software assurance are equivalent concepts [true/false]

6,Code Signing does not help in providing ? a) The application/code can be trusted b) integrity of the data c) avoid namespace conflicts d) verify the identity of the author.

7,6. Asymmetric key encryption often is used to exchange a symmetric key.
T/F

8,When we have to send a large amount of data, what should be used to ensure secure transmission. Select most appropriate.
a) Digital Signature.
b) Symmetric Encryption.
c) Asymmetric Encryption.
d) Combination of all a) & b) & c)
e) Combination of b) & c)

9,Question 1- To prevent abrupt application termination and to detect and recover from errors in software, which of the following is the BEST mechanism to use? Select the most appropriate.

a- Assertions
b- Programmatic checks (eg- try-catch-finally)

c- Stack traces
d- Debugger

Question 2- When engaging in the process of threat modelling, an example of a threat is: Select the most appropriate.

a- an undesirable outcome from a series of actions.
b- a user that has malicious intent
c- a known vulnerability
d- a missing security control

10,In an application bugs and flaws usually occur in the ratio of ?
a) 40:60
b) 60:40
c) 75:25
d) 50:50

11,(Multiple Choice) Which of the mobile OS does not support application sandboxing ?
a. iOS,
b. Android,
c. Windows,
d. Nokia Symbian

12, Whitelists should be used only as a secondary defense, a blacklist should be used wherever possible (T/F)

13,Q) SSL uses both symmetric and asymmetric cryptography.
a) True
b) False

14,T or F: In an Attack Tree, if a parent node has only OR-type children nodes, then the cost of the parent node is sum of the costs of the children nodes.

15,In production environment, a detailed logging of anomalous system behavior should be carried out at __________ level.
a. INFO b. CRITICAL c. DEBUG d. ERROR

16,Which of these is NOT a way to prevent Log Injection attack
a. Encode special characters
b. Cryptographic hash for each log entry
c. Single log file at shared server location
d. Add a sequence number with each message

17,Changing passwords frequently could do more harm than good. True/ False

18,Your organization wants to share information with multiple parties secretly. Which cryptographic primitive would you use?

i) Symmetric Encryption
ii) Asymmetric Encryption
iii) Hashing
iv) MAC codes

19,Which threat can be prevented by having unique usernames generated with a high degree of entropy? a. Crypt-Analysis of hash values b. Spamming c. Authentication Bypass d. Authorization Bypass

20,Data Encryption Standard or DES proposed in '75 in the federal register had 64 bits key size.
True/False

21,In Eddie Bauer Data Breach, hackers hacked into which systems:
1. Internal computer systems, to which its point-of-sale terminals were connected.
2. Computer systems that handle profile data of the frequent customers.
3. Computer systems that contain the price details of commodities.

22,In case of Message Authentication Codes same key is used to sign and verify the data
True/False

23,Which Encryption modes when using block ciphers should not be used when encrypting data
a) Counter
b) Ciper Feedback
c) Cipher-block chaining
d) Electronic Codebook

24,T/ F Client side validation of every input form field ensures that no malformed input will be sent to the server.

25,What is the prisonerâ€™s dilemma meant to illustrate?
A) It is better to always think selfishly
B) It is better to cooperate with others
C) There is always a good cop and a bad cop
D) It is better to confess.

26,From security perspective which of the following is an ideal message?

com.ncsu.login.exception: Invalid credentials
Invalid password supplied three times
Invalid username or password: Please call 1-800-XXX-XXXX for help
Username is valid but invalid password entered. Try again!

27,Which ones are script kiddies/amateur hackers? (Select all that apply)
1. That attack against users (bribery, theft, etc)
2. Mathematical attacks against algorithms (related-key attacks etc)
3. General attacks against implementations (reading memory, reverse engineering etc.)

28,ElGamal encryption is a secure algorithm because,(Select the most appropriate)
a) Key size is huge.
b) Because no efficient algorithm currently exists for factoring large numbers.
c) Because no efficient algorithm currently exists to calculate discrete logarithms.
d) Both b) and c)

29,1. How security and reliability are related as per the views expressed by Fred Schneider?
a. The security of any software system is adversely affected if there are efforts made to enhance the reliability of the system.
b. The software system tends to fail more often if security features are implemented in the system as components cannot have security features and recovery ability built them into at the same time.
c. Increasing the reliability of the system through resource or component replication has no effect on securing the system as the attack surface of the system doesnâ€™t get reduced; it rather increases due to replication.
d. Enhancing the reliability of the software system, makes the system more secure as reliability features be default implements certain security configurations.

30,Digital signature ensures that
A. message was created by a known sender (authentication)
B. sender cannot deny having sent the message (non-repudiation)
A
B
Both A & B
Neither A nor B

31,T/F An initialization vector is a value used to generate completely different cipher texts each time even when encrypting the same plaintext multiple times.

32,Security vulnerabilities can be identified using techniques that can be broadly classified as static or dynamic. Column A lists these techniques. Match Column A with Column B.

	Column A		Column B
1.	Fuzzing Testing	A.	Static Techniques
2.	Lexical Analysis	B.	Dynamic Techniques
3.	Pattern Matching		
4.	Input Sanitisation		
5.	Data Flow Analysis		
6.	Parsing		

33,Which is the following is NOT a step in the SSL/TLS handshake process?
a. The server sends its public key certificate to the client.
b. The client generates a random symmetric key.
c. The client encrypts the symmetric key with its private key.
d. The server decrypts the symmetric key using its private key.

34,Which Security property specifies that a user canâ€™t perform an action and later deny performing it
a)Authentication
b) Non-repudiation
c) Confidentiality
d) Integrity

35,Use of encryption algorithms to protect data integrity is encouraged.

36,[True/False] Hash function transforms data to make it unreadable to anyone except those possessing a key.

37,Reusing Electronic Codebook mode (ECB) to encrypt the same plain text block produces different cipher texts each time. (T/F)

38,Which of the following consequences is most likely to occur due to an injection attack?
1. Spoofing
2. Insecure direct object references
3. Denial of service
4. None of the above

39,Abuse cases are interactions between actors and the system that result in harm to the system or its stakeholders.
A. True
B. False

40,Which of following are best practices when using cryptography? Select all that apply.
A.	Use proprietary cryptographic algorithms.

B.	Pay attention to key lengths.
C.	Do not use widely distributed secrets.
D.	Use only unconditionally secure algorithms.

41,(T/F)
The best way to use Cryptography in our design is by rolling our own cryptographic algorithms or implementation so that attackers cannot guess the underlying algorithm used and exploit it using known methods.

True or False

42,Certificate Authority (CA) is responsible for signing public keys. (T/F)

43,In computer security, â€_â€_â€_. means that computer system assets can only be modified only by authorized parities.
A) Confidentiality
B) Integrity
C) Availability
D) Authenticity

44,ElGamal encryption system is a symmetric key encryption algorithm. (T/F)

45,Which of the following is incorrect regarding â€˜saltâ€™?

a)	The salt should be kept secret.
b)	Salt is a randomized string added to the password
c)	Salt can either be appended or prepended
d)	It is better not to generate the same salt for the same password again.

46,What threat arises when HTTP cookies with tokens are not flagged as secure?
a. Session Replay
b. Session Fixation
c. Session Hijacking
d. Access Control Violation

47,Which is not one of the Block Cipher modes of Operation ?   a) Electronic Code Book (ECB) Mode   b) Cipher Block Chaining (CBC) Mode   c) Cipher Feedback (CFB) Mode   d) Block Chain Mode (BCB) Mode

48,The Snapchat breach was because of: A. State sponsored Actor B. Phishing Attack C. Point of Sale Malware attack D. None of the above

49,Which of the following are cryptographic goals?
a) Confidentiality b) Data Integrity c) Authentication d) Authorization

50,Which of following is Not/Incorrect as per OWASP Password Guideline:
A. Atleast 1 Uppercase and 1 LowerCase.
B. Atleast 8 Characters
C. Atleast 1 digit and 1 special Character
D. Atmost 128 characters.

51,[Multiple choice Question]
Which of the following can be used as possible solutions to buffer overflow attack?
- Filter user input
- Two factor authentication
- Encryption mechanisms
- Implement Address space layout randomization
- Using Stack Canaries

52,Which of the following is a cause of insecure cryptography? (A) Unsalted Hash (B) Unsafe Key Generation and Storage (C) Failure to rotate keys (D) Failure to encrypt sensitive information (E) All of the above are insecure practices

53,Which of the following are true about passwords?

1. Password expiration policies frequently frustrate users, who then, tend to choose weak passwords and use the same few passwords for many accounts

2. People are better at remembering passphrases as passwords than pronounceable passwords

3. It is much easier to crack new passwords if old passwords had been cracked before

54,Limited memory, lower computing power, and funcitonality makes mobile devices a difficult target
a. True
b. False

55,Q. Which one of the following algorithm is not used in asymmetric-key cryptography?
a) RSA algorithm
b) diffie-hellman algorithm
c) electronic code book algorithm
d) none of the mentioned

56,Cross-site request forgery prevention tokens should have which of the following?
a) Token is cryptographically random
b) Token is reused each time a user accesses the site
c) Token is associated with a particular user session
d) Token is stored in a secure cookie

57,Which of the following are true regarding logging practices?
a)Can write sensitive information into log files.
b)Copies of log files should be made at regular intervals
c)Excessive logging can provide cover for an attacker while attempting to penetrate a system
d)Should not log administration events and access control events

58,1.In the sandbox mechanism, an application can not allow another application to get access to its resources.(T/F)
2.Apple iOS gathers permissions at run time while Google Android OS does it all the time.(T/F)

59,As per OWASP recommendation session id lengths should be minimum 8 bytes?
True/False

60,T/F: According to Fred Schneider, using a different compiler or instruction set is a good example of diversity to make systems reliable and attack-resistant.

61,An attacker lures a victim to malicious content on a Web site. A request is automatically sent to the vulnerable site which includes victimâ€™s credentials. This attack is:

a) Cross Site Scripting Attack.
b) Cross Site Forgery Attack.
c) Broken Authentication.
D) Phising.

62,If an attacker gets the ability to force the server to make GET request, what all can the attacker do:-
i) File disclosure
ii) Denial of service
iii) Attack internal systems behind firewall
iv) port scanning of internal network
v) all of the above
vi) none of the above

63,Microsoft STRIDE (six) threat categories include:

*Information disclosure
*Random Sessions
*Elevation of privilege
*Tracking actions

64,An organization is as strong as its weakest link. To hack into an organization, the weakest link is the Wi-Fi, if it offers an open Wi-Fi access to anyone entering its premise. (T/F)

65,Which of the following MUST NOT be used to authenticate public keys? Select the most appropriate:
A. Public key Infrastructure
B. Asymmetric Encryption
C. Identity-Based Cryptography
D. Web of trust

66,When should password encryption be used?

i) Should never be used. Always use Hash
ii) To retrieve password from external system
iii) Should never be used. Store in database as plaintext

67,Which of the following is the best way to prevent unvalidated redirect and forwards vulnerabilities?
1. Use an allow list, such as table indirection
2. Use client-side validation.
3. Use session-based indirection
4. None

68,Which of the following methods may be effective in testing for the use of components with known vulnerabilities?
a) Use of Security Wrappers around components
b) Static code analysis Scanning
c) Manually reviewing code and researching components
d) Establishing security policies governing component use

69,Session IDs are used to identify a user that has logged into a website and hence can be used to hijack the session and get privileged access. True /False

70,Find the Odd One:

A. Encryption <--> Confidentiality
B. MAC <--> Integrity
C. Digital Signature <--> Availability
D. Firewall <--> Security

71,In Chandu Ketkarâ€™s words, Medical technology is not as secure as financial technology in the present day world. Which of the following are reasons for it ?

72,Hash Function can not Provide Basic cryptographic services such as Confidentiality,Authentication on their own. T/F?

73,While making a decision on the type of encryption mode to be used for storing confidential data, if the application requires random access to this data, Block Ciphers in counter mode should not be used. (T/F)

74,Q) Which one of the following cryptographic primitives provide only data integrity and not non-repudiation?
i) Digital signature
ii) Symmetric Encryption
iii) Asymmetric Encryption
iv) Message Authentication codes

75,Entity Authentication and non-repudiation can be achieved by digital signatures.
a.) True.
b.) False.

76,Which of the following are examples of Asymmetric key algorithms
AES
RSA
Triple DES
ElGamal
Elliptic Curve Digital Signature Algorithm
Blowfish

77,(T/F) Block ciphers are considered more secure than stream ciphers because they are more random.

78,Which of the following are important considerations when designing a cryptographic control for your application? multiple options can be true
a. use symmetric keys that are at least 112 bits in length
b. us the highest level protocol to avoid mistakes
c. ensure that performing regular key rotation is possible and convenient
d. use a hard-coded secret as a failsafe mechanism in case other controls are broken

79,ElGamal encryption system is
a) symmetric key encryption algorithm
b) asymmetric key encryption algorithm
c) not an encryption algorithm
d) none of the mentioned

80,Type: True/False Question: Logging a failed Login attempt is not necessary.

81,Session rotation and session timeout provides better security and usability. True / False

82,Which of the following is a typical use of hash function? Select the most appropriate:
a. Protecting the confidentiality of usernames.
b. Protecting the integrity of usernames.
c. Protecting the confidentiality of passwords.
d. Protecting the integrity of passwords.

83,Which of the following is not one of the major steps included in the three-pronged attack described by Verizon in its 2016 data breach investigation?
A) Downloading malware into an individual's PC.
B) Using credentials obtained to launch further attacks.
C) Obtaining sensitive information stored in the compromised system.
D) Sending a phishing email to the victim.

84,(T/F) The classical triad of information security: confidentiality, integrity, availability.

85,Proprietary cryptographic algorithms are almost always weaker than standard cryptographic algorithms because they are not widely peer reviewed and not designed by cryptographers.

1. True
2. False

86,Which is the best method to protect web browser cookies?
a. Encrypt the cookie.
b. Hash the contents of the cookie.
c. Set the secure flag at the server side.
d. Certify the cookie.

87,(Multiple Choice)
Recently a spyware product called Pegasus was developed that takes advantage of three zero-day exploit in iOS to jailbreak iOS devices. From the given list, choose the flaws in iOS that were being exploited by the malware:

a. A kernel base mapping vulnerability
b. Buffer Overflow in iOS FontParser class
c. A flaw in the Safari WebKit
d. An iOS camera application vulnerability
e. A kernel memory corruption flaw

88,(T/F) If the verb describes mechanical interaction with the software interface, then the event is a mandatory log event.

89,Threat Modeling is used to Identify potential security issues even before writing any code. (True/False)

90,The Pegasus attack is highly configurable and is designed to spy on text messages , calls, emails. a. True b. False

91,MAC and Digital Signatures ensure that given website belongs to a trusted organization and material downloaded from the Internet originated from a trusted organization: True/False?

92,Type:True/False Question: Session rotation (reassign session ID periodically) and Session timeout gives a balance between security and usability.

93,Multiple choice question:
Software security defects come into which of the following two categories:
1. Bugs
2. Flaws
3. Errors

94,While inspecting OpenMRS, you see a stack trace on the screen in response to the bad data you submitted. This is a violation of which principle of secure design? 1) Principle of least privilege 2) Compartmentalization 3) Fail and Recover Securely 4) Defense in Depth

95,which of the following is true?
*Symmetric Cryptography is typically used to transport Asymmetric keys
*Asymmetric Cryptography is typically used to transport Symmetric keys

96,True/False question:
Asymmetric algorithms are much slower than Symmetric algorithms.
True
False

97,Which of the following is not in the CSD's Top 10 list to avoid Security Design Flaws ?
a) Authorize after you authenticate
b) Log access control and administration events
c) Use Cryptography correctly
d) Always consider users

98,What type of vulnerability is the following code prone to?

```
String query = "SELECT * FROM users WHERE userid = ?";
PreparedStatement st = connection.prepareStatement(query);
st.setString( 1, request.getParameter("uid"));
ResultSet rs = st.executeQuery( );
```

- SQL Injection

- Insecure Direct Object References
- Security Misconfiguration
- Missing function level access control

99,Which of the following attack patterns would likely be the most pressing concerns when dealing with distributed architecture?
a) Parameter Manipulation attacks
b) Replay attacks
c) Session Management attacks
d) Sniffing attacks

100,Which of the following attack Strings may be used to exploit an insecure direct object Reference? <More than one correct answer may be possible>

A. ' or 1 = 1; --
B. ../../../etc/passwd
C. %PATH%/apache/bin/passwd
D. <script>window.close()</script>
E. All of these
F. None of These

101,According to NIST (National Institute of Standards and Technology), minimum key-length for RSA algorithm for the time period 2011-2030 has been set as:
a) 256 bits   b) 512 bits c) 1024 bits d) 2048 bits

102,What is the maximum number of enities that should be allowed to share the public half of an asymmetric key pair?
Choices:
1
2
10
infinite

103,Having the same initialization vector during multiple instances while encrypting block ciphers is advised and prevents information leaks to attackers(T/F)

104,A commonly used "secure" symmetric cryptographic algorithm is?

- Triple-DES
- RC2
- AES
- RSA

105,T/F: Symmetric encryption algorithms works faster and is relatively simple to implement than asymmetric encryption algorithms

106,Multiple choice checkbox(select all that apply): When attempting

to enhance the software development life cycle in order to produce more secure software, which of the following activities should be used?
a) Penetration testing
b) Abuse cases
c) Firewall egress configuration
d) Code review

107,1.which of the following technique(s) is/are involved in mitigating buffer overflow attacks.

a. Address space layout randomization
b. Stack Canaries
c. Data Execution Prevention
d. All the above

108,(Multiple Choice)

Recently a spyware product called Pegasus was developed that takes advantage of three zero-day exploit in iOS to jailbreak iOS devices. From the given list, choose the flaws in iOS that were being exploited by the malware:

a. A kernel base mapping vulnerability
b. Buffer Overflow in iOS FontParser class
c. A flaw in the Safari WebKit
d. An iOS camera application vulnerability
e. A kernel memory corruption flaw

109,(T/F) A hash that is created from a set of data can be reversed.

110,Which of following property contribute to make a session identifier secure?
A.   Uniqueâˆ_
B.   Non-guessableâˆ_
C.   Non-readable
D.   Cryptographic

111, ______ is/are used to verify the authenticity of the websites.

a.) Digital Signatures.
b.) Message Authentication Codes.
c.) Both.
d.) None.

112,Which of the following should never be recorded in logs?

Passwords
Credit Card numbers
Usernames

IP Addresses

113,According to Leigh Honeywell, Senior Staff Security Analyst at Slack, the concept of uniformity is to be designing exiting, innovative agile security workaround. F

114,1. Strictly as a comparison of both of the Silver Bullet Podcasts, a major difference in the time during Marty E. Hellmanâ€™s days as an active researcher and Katie Moussouris current work is:
a. Involvement of Cyber Security in Day-to-Day Lives
b. Approach to Cryptography
c. Role of Security in the Software Development Lifecycle
d. Perception towards Peer Reviewed Security

115,2. Select the correct statement/statements pertaining to symmetric and asymmetric key encryption.
a. Asymmetric key encryption uses two private keys â€“ one to be used for encryption and the other used for decryption and are only shared in between two users.
b. Asymmetric key encryption is often used to encrypt and share the private key used in symmetric key encryption.
c. Asymmetric key encryption is slower compared to symmetric key encryption.
d. Symmetric key encryption consists of one public key and one private key components to be used in encryption and decryption respectively.

116,Which of the following are cryptographic goals? Select all that apply:
A. Confidentiality
B. Data Integrity
C. Authentication
D. Authorization

117,The typical use of a hash function is to protect the integrity of usernames? True or False

118,Which of the following regarding initialization vectors are true? Select all that apply.
1. Do not use initialization vectors.
2. Always reuse initialization vectors.
3. An initialization vector is a value used to generate completely different cipher texts each time, even when encrypting the same plaintext multiple times.
4. An initialization vector is a value used to generate same cipher texts each time, even when encrypting the same plaintext multiple times.

119,Which of the following is not a Secure Design Guidelines

1. Securing the Weakest Link
2. Separation of Privilege
3. secure by default
4. show error messages

120,Below Techniques can be used when the data does not need to be decrypted and can be kept stored in it's encrypted form
a) Hash Functions
b) Asymmetric Key Encryption
c) Message Authentication Codes
d) Digital Signatures

121,Q1. Which of the following are correct combinations of attacker type and their corresponding typical threat
a) Criminals attacks against users
b) Script kiddies or amateur hackers carry out attacks against implementations
c) Government Agencies pose mathematical attacks against algorithms
d) Dedicated hackers pose cryptanalytic attacks against implementations

122,The correct share of design and implementation flaws in industry is (multiple choice):
20%: 80%
30%: 70%
40%: 60%
50%: 50%

123,Hash function can be used for storing passwords or protecting message integrity

124,Network encryption protocol (such as IPSec or SSL) protects data in transit. What kind of encryption does it use?
Options: Asymmetric; Symmetric; Both symmetric and asymmetric?

125,(T/F) Asymmetric key encryption is typically faster than symmetric key encryption.

126,[True or False] Excessive data logging can hinder a system administrator's ability to detect anomalies.

127,Q. Voice privacy in GSM cellular telephone protocol is provided by
a) A5/2 cipher
b) b5/4 cipher
c) b5/6 cipher
d) b5/8 cipher

128,Which cryptographic primitive provides data integrity and non-repudiation services?

Choices:
Encryption
Hash Functions
Message Authentication Codes
Digital Signatures

129,How many of the following tools can be used to perform Penetration Testing?
1. Metasploit
2. Cain and Abel
3. ELK (Elasticsearch, Logstash, Kibana)
4. Wireshark

Options:
A. 1
B. 2
C. 3
D. 4

130,Which of the following mechanisms are likely to help mitigate SQL injection attacks?
A. Use of stored procedures
B. Use of ad-hoc queries
C. Use of parameterized queried
D. Use of input validation

131,Which of the following attacks can be used to by-pass any kind of client side input validation?
A. SQL injection attack
B. Man-in-the-middle attack
C. Session hijacking attack
D. Both A and B

132,Security vulnerabilities are categorized into Implementation bugs and Architecture flaws.
Count the number of implementation bugs in the below list of vulnerabilities:

i)   Duplicated code
ii)   Classic buffer overflow
iii)   Unsafe system calls
iv)   Broken access control
v)   Incorrect input validation
vi)   Privileged block protection failure (DoPrivilege() method in Java)

Choose the correct option:
a)   2 bugs or fewer
b)   3 bugs
c)   4 bugs

d) 5 or more bugs

133,What are the problem(s) that ketkar(in cigital talk) typically finding in todayâ€™s medical devices about security?
A. Some of them are too old that need to do security defense like encryption.âˆ_
B. The operations of the device are not pragmatic. âˆ_
C. They donâ€™t notice the privacy concern. âˆ_
D. The devices always have authentication, but it too wasting time to use it.

134,Input/Output filtering are some ways ways of mitigating Cross Site Scripting. True/False?

135,(T/F) It is a good practice to include index.html files in all directories ?

136,After retiring from comedy, Seinfeld is now a UI/UX developer at a startup that rents out puppies for the day (Rent-A-Puppy). As a developer, all he has to do is to design a table for the different rates. Here are some highlights of his day:
1. He logs in to his administrator account, checks out what puppies are available today and then makes sure his friend Elaine gets the best pick
2. While being logged in, he clicks on several ads promising him $7000 while sitting at home. When he gets back to his account with Rent-A-Puppy, it is strangely logged out.
3. George visits him in his office to find Seinfeld has gone home. George tries to login to Seinfeldâ€™s account using his name and â€œrentapuppyâ€ù as a password. Now, George is also able to get his best pick.
4. While waiting for the $7000 at home, Seinfeld writes some code and sends the code to his boss on his Gmail account.
While it is kind of obvious that a system should not be as insecure as the above, which of the above represents a Security Misconfiguration in the system?
a) 1,4
b) 1,3
c) 1,3,4
d) 1,2,3

137,Initialization Vector is a value used to generate completely different ciphertexts each time even when encrypting the same plaintext multiple times.
A. True
B. False

138,(T/F)
The HttpOnly flag indicates that the cookie should not be available to the client script.

139,Initiative vector don't need to be random or kept secret

140,Hash function is typically used for? Select the best choice.
a) Protecting the confidentiality of usernames.
b) Protecting the integrity of usernames.
c) Protecting the confidentiality of passwords.
d) Protecting the integrity of passwords.

141,Which of the following offers perfect secrecy?
a. Asymmetric Encryption
b. Stream Cipher
c. One Time Pad
d. Block Cipher

142,Which of following is good policies for the password? Select all that apply.
A. Use a very complex pattern for password
B. Use a long password which is easy for you to remember.
C. Create password based on things that make us happy
D. Always reuse their old password.

143,What is the maximum number of entities that should be allowed to share the private half of an asymmetric key pair?
a. one
b. two
c. three
d. infinite