1.	Asymmetric Encryption: Why can a message encrypted with the Public Key only be decrypted with the receiver's appropriate Private Key? 1. Not true, the message can also be decrypted with the Public Key. 1. 2. A so called "one way function with back door" is applied for the encryption. 2. The Public Key contains a special function which is used to encrypt the message and which can only be reversed by the appropriate Private Key. 3. 4. The encrypted message contains the function for decryption which identifies the Private Key.	2
2.	In which way does the Combined Encryption combine symmetric and asymmetric encryption? 1. First, the message is encrypted with symmetric encryption and afterwards it is encrypted asymmetrically together with the key. 2. The secret key is symmetrically transmitted, the message itself asymmetrically. 3. First, the message is encrypted with asymmetric encryption and afterwards it is encrypted symmetrically together with the key. 4. The secret key is asymmetrically transmitted, the message itself symmetrically.	4
3.	Which is the largest disadvantage of the symmetric Encryption? 1. More complex and therefore more time-consuming calculations. 2. Problem of the secure transmission of the Secret Key. 3. Less secure encryption function. 4. Isn't used any more.	2
4.	Which is the principle of the encryption using a key? 1. The key indicates which funcion is used for encryption. Thereby it is more difficult to decrypt a intercepted message as the function is unknown. 2. The key contains the secret function for encryption including parameters. Only a password can activate the key. 3. All functions are public, only the key is secret. It contains the parameters used for the encryption resp. decryption. 4. The key prevents the user of having to reinstall the software at each change in technology or in the functions for encryption.	3
5.	A substitution cipher substitutes one symbol with 1. Keys 2. Others 3. Multi Parties 4. Single Party	2

6.	An asymmetric-key (or public-key) cipher uses 1. 1 Key 2. 2 Key 3. 3 Key 4. 4 Key	2
7.	A straight permutation cipher or a straight P-box has the same number of inputs as 1. cipher 2. Frames 3. Outputs 4. Bits	3
8.	We use Cryptography term to transforming messages to make them secure and immune to 1. Change 2. Idle 3. Attacks 4. Defend	3
9.	The man-in-the-middle attack can endanger the security of the Diffie-Hellman method if two parties are not 1. Authenticated 2. Joined 3. Submit 4. Separate	1
10.	The cryptography algorithms (ciphers) are divided into 1. two groups 2. four groups 3. one single group 4. None	1
11.	The shift cipheris sometimes referred to as the 1. Caesar cipher 2. Julia cipher 3. plain cipher 4. All of them	1

12.	One commonly used public-key cryptography method is the ______ algorithm. 1. RSS 2. RAS 3. RSA 4. RAA	3
13.	A(n) ______ algorithm transforms cipher text to plaintext. 1. encryption 2. decryption 3. either (a) or (b) 4. neither (a) nor (b)	2
14.	The ________ method provides a one-time session key for two parties. 1. Diffie-Hellman 2. RSA 3. DES 4. AES	1
15.	A(n) ______ is a keyless substitution cipher with N inputs and M outputs that uses a formula to define the relationship between the input stream and the output stream. 1. S-box 2. P-box 3. T-box 4. none of the above	1
16.	A ________ cipher replaces one character with another character. 1. substitution 2. transposition 3. either (a) or (b) 4. neither (a) nor (b)	1
17.	The ________ cipher reorders the plaintext characters to create a ciphertext. 1. substitution 2. transposition 3. either (a) or (b) 4. neither (a) nor (b)	2

18.	_______ is a round cipher based on the Rijndael algorithm that uses a 128-bit block of data. 1. AEE 2. AED 3. AER 4. AES	4
19.	The _________ attack can endanger the security of the Diffie-Hellman method if two parties are not authenticated to each other. 1. man-in-the-middle 2. ciphertext attack 3. plaintext attack 4. none of the above	1
20.	A combination of an encryption algorithm and a decryption algorithm is called a ________. 1. cipher 2. secret 3. key 4. none of the above	1
21.	AES has _____ different configurations. 1. two 2. three 3. four 4. five	3
22.	DES is a(n) ________ method adopted by the U.S. government. 1. symmetric-key 2. asymmetric-key 3. either (a) or (b) 4. neither (a) nor (b)	1
23.	DES uses a key generator to generate sixteen _______ round keys. A) 32-bit B) 48-bit C) 54-bit D) 42-bit	2

24.	The Caesar cipher is a ________cipher that has a key of 3. 1. transposition 2. additive 3. shift 4. none of the above	3
25.	ECB and CBC are _________ ciphers. 1. block 2. stream 3. field 4. none of the above	1
26.	A(n) ________is a keyless transposition cipher with N inputs and M outputs that uses a table to define the relationship between the input stream and the output stream. 1. S-box 2. P-box 3. T-box 4. none of the above	2
27.	_________ DES was designed to increase the size of the DES key. 1. Double 2. Triple 3. Quadruple 4. none of the above	2
28.	DES has an initial and final permutation block and __________ rounds. 1. 14 2. 15 3. 16 4. none of the above	3
29.	The DES function has ________ components. A) 2 B) 3 C) 4 D) 5	3

30.	In a(n) ________ cipher, the same key is used by both the sender and receiver. 1. symmetric-key 2. asymmetric-key 3. either (a) or (b) 4. neither (a) nor (b)	1
31.	The _______ cipher is the simplest monoalphabetic cipher. It uses modular arithmetic with a modulus of 26. 1. transposition 2. additive 3. shift 4. none of the above	3
32.	In a(n) ________, the key is called the secret key. 1. symmetric-key 2. asymmetric-key 3. either (a) or (b) 4. neither (a) nor (b)	1
33.	RSA stands for: 1. Rivest Shamirand Adleman 2. Rock Shane and Amozen 3. Rivest Shane and Amozen 4. Rock Shamir and Adleman	1
34.	The S-Box is used to provide confusion, as it is dependent on the unknown key. 1. True 2. False	1
35.	In the DES algorithm, although the key size is 64 bits only 48bits are used for the encryption procedure, the rest are parity bits. 1. True 2. False	2
36.	In the DES algorithm the round key is ___________ bit and the Round Input is _____________bits. 1. 48, 32 2. 64,32 3. 56, 24 4. 32, 32	1

37.	In the DES algorithm the Round Input is 32 bits, which is expanded to 48 bits via _____________ 1. Scaling of the existing bits 2. Duplication of the existing bits 3. Addition of zeros 4. Addition of ones	1
38.	The Initial Permutation table/matrix is of size 1. 16×8 2. 12×8 3. 8×8 4. 4×8	3
39.	In the DES algorithm the 64 bit key input is shortened to 56 bits by ignoring every 4th bit. 1. True 2. False	2
40.	AES uses a _____________ bit block size and a key size of ___________ bits. 1. 128; 128 or 256 2. 64; 128 or 192 3. 256; 128, 192, or 256 4. 128; 128, 192, or 256	4
41.	SHA-1 produces a hash value of 1. 256 bits 2. 160 bits 3. 180 bits 4. 128 bits	2
42.	The big-endian format is one in which 1. the least significant byte is stored in the low-address byte position 2. the least significant byte is stored in the high-address byte position 3. the most significant byte is stored in the high-address byte position 4. the most significant byte is stored in the low-address byte position	4
43.	Caesar Cipher is an example of 1 Poly-alphabetic Cipher 2 Mono-alphabetic Cipher 3 Multi-alphabetic Cipher 4 Bi-alphabetic Cipher	2

44.	DES using 56 bits 1. Cannot be broken in given time using presently available computers. 2. Can be broken only if algorithm is known using even slow computers. 3.Can be broken by presently available high speed computers. 4. It is impossible to break.	3
45.	Triple DES 1. Cannot be broken in given time using presently available computers. 2. Can be broken only if algorithm is known using even slow computers. 3.Can be broken by presently available high speed computers. 4. It is impossible to break.	1
46.	The Acronym DES stands for 1.Digital Evaluation System. 2.Digital Encryption System. 3.Digital Encryption Standard. 4.Double Encryption System.	2
47.	The Acronym AES stands for 1.Advanced Encryption Standard 2.Advanced Encryption System. 3.Advanced Evaluation System. 4. Advanced Evaluation Standard	1
48.	Triple DES 1. Is a Symmetric Key Encryption method. 2.Gurantees Excellent Security 3.Is implementable as hardware VLSI chip. 4.Is a public key encryption method	2