|  |  |
| --- | --- |
| How many keys exist in a public/private key pair?   1. 1 2. 2 3. 3 4. 4 | [Two keys, a public key and a private key, exist in a key pair.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=424028117&rowid=430&noteMenuToggle=0&leftMenuState=1#answer.N14) |
| **2.** | How many keys are needed for symmetric key encryption?   1. 1 2. 2 3. 3 4. 4 | [The same key is used to encrypt and decrypt the data with symmetric key encryption.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=424028117&rowid=430&noteMenuToggle=0&leftMenuState=1#answer.N39) |
| **3.** | Which of the following key lengths would be considered uncrackable? (Choose all that apply.)   1. 512 2. 256 3. 128 4. 64 | [A key length of 256 bits or more is considered uncrackable.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=424028117&rowid=430&noteMenuToggle=0&leftMenuState=1#answer.N64) |
| **4.** | What algorithm outputs a 128-bit message digest regardless of the length of the input?   1. SHA 2. MD5 3. RC4 4. RC6 | [MD5 outputs a 128-bit digest with variable-length input.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=424028117&rowid=430&noteMenuToggle=0&leftMenuState=1#answer.N89) |
| **5.** | What algorithm outputs a 160-bit key with variable-length input?   1. SHA 2. MD5 3. RC4 4. RC6 | [SHA outputs a 160-bit key with variable-length input.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=424028117&rowid=430&noteMenuToggle=0&leftMenuState=1#answer.N114) |
| **6.** | Which algorithm is used in the digital signature process?   1. RC4 2. RC5 3. Blowfish 4. MD5 | [MD5 is used in the digital signature process.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=424028117&rowid=430&noteMenuToggle=0&leftMenuState=1#answer.N139) |
| **7.** | What is cryptography?   1. The study of computer science 2. The study of mathematics 3. The study of encryption 4. The creation of encryption algorithms | [Cryptography is the study of encryption.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=424028117&rowid=430&noteMenuToggle=0&leftMenuState=1#answer.N164) |
| **8.** | What is the process of changing the order of some characters in an encryption key?   1. Transposition 2. Subtraction 3. Substitution 4. Transrelation | [Transposition is the process of changing the order of some characters in an encryption process.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=424028117&rowid=430&noteMenuToggle=0&leftMenuState=1#answer.N189) |
| **9.** | Data encrypted with the server's public key can be decrypted with which key?   1. The server's public key 2. The server's private key 3. The client's public key 4. The client's private key | [Data can be decrypted with the other key in the pair-in this case, the server's private key.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=424028117&rowid=430&noteMenuToggle=0&leftMenuState=1#answer.N214) |
| **10.** | Which type of encryption is the fastest to use for large amounts of data?   1. Symmetric 2. Public 3. Private 4. Asymmetric | [Symmetric key encryption is fast and best to use when you have large amounts of data.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=424028117&rowid=430&noteMenuToggle=0&leftMenuState=1#answer.N239) |
| **11.** | What is the goal of a known–plain text attack?   1. To read the encrypted data 2. To gain access to the public key 3. To discover the encryption key 4. To validate the sender of the data | [The goal of a known plain text attack is to discover the encryption key.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=424028117&rowid=430&noteMenuToggle=0&leftMenuState=1#answer.N264) |
| **12.** | Which cryptographic attack attempts to crack the code by looking for patterns and using statistical analysis?   1. Cipher text–only attack 2. Chosen–plain text attack 3. Chosen–cipher text attack 4. Brute-force attack | [A cipher text only attack attempts to crack the encryption using cryptoanalysis.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=424028117&rowid=430&noteMenuToggle=0&leftMenuState=1#answer.N289) |
| **13.** | Which two factors are of concern when using brute-force attacks against encryption?   1. Time 2. Money 3. Knowledge of the sender 4. The ability to capture data | [Time and money are the two biggest concerns when attempting to break encryption using a brute-force method.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=424028117&rowid=430&noteMenuToggle=0&leftMenuState=1#answer.N314) |
| **14.** | Which program is useful in ensuring the integrity of a file that has been downloaded from the Internet?   1. Tripwire 2. Norton Internet Security 3. Snort 4. WinMD5 | [WinMD5 can be used to verify the integrity of a file downloaded from the Internet.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=424028117&rowid=430&noteMenuToggle=0&leftMenuState=1#answer.N339) |
| **15.** | What are some of the common fields in an x.509 certificate? (Choose all that apply.)   1. Secret Key 2. Expiration Date 3. Issuer 4. Public Key | [An x.509 certificate includes a field for Issuer and Public Key.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=424028117&rowid=430&noteMenuToggle=0&leftMenuState=1#answer.N364) |
| **16.** | What is the standard format for digital certificates?   1. x.500 2. x.509 3. x.25 4. XOR | [x.509 is the standard for digital certificates.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=424028117&rowid=430&noteMenuToggle=0&leftMenuState=1#answer.N389) |
| **17.** | What would the cipher text result be of a value of 1 in plain text and 0 in the secret key after an XOR process?   1. 1 2. 0 | [Different values such as 1 and 0 in an XOR process result in a value of 1.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=424028117&rowid=430&noteMenuToggle=0&leftMenuState=1#answer.N414) |
| **18.** | What are two components of a PKI?   1. User passwords 2. Digital certificates 3. Encrypted data 4. CA | [CA (certificate authorities) and digital certificates are two components of a PKI.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=424028117&rowid=430&noteMenuToggle=0&leftMenuState=1#answer.N433) |
| **19.** | What element of the CIA triad ensures that the data sent is the same data received?   1. Confidentiality 2. Integrity 3. Authentication | [Integrity ensures the data is not modified in transit.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=424028117&rowid=430&noteMenuToggle=0&leftMenuState=1#answer.N458) |
| **20.** | What is the purpose of a hash?   1. To ensure confidentiality when using a public network such as the Internet 2. To ensure integrity of a transferred file 3. To ensure only authorized users are accessing a file 4. To ensure the data is available to authorized users | [A hash is a one-way encryption used to validate the integrity of a file.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=424028117&rowid=430&noteMenuToggle=0&leftMenuState=1#answer.N480) |

**Answers**

|  |  |
| --- | --- |
| **1.** | Two keys, a public key and a private key, exist in a key pair. |
| **2.** | The same key is used to encrypt and decrypt the data with symmetric key encryption. |
| **3.** | A key length of 256 bits or more is considered uncrackable. |
| **4.** | MD5 outputs a 128-bit digest with variable-length input. |
| **5.** | SHA outputs a 160-bit key with variable-length input. |
| **6.** | MD5 is used in the digital signature process. |
| **7.** | Cryptography is the study of encryption. |
| **8.** | Transposition is the process of changing the order of some characters in an encryption process. |
| **9.** | Data can be decrypted with the other key in the pair—in this case, the server's private key. |
| **10.** | Symmetric key encryption is fast and best to use when you have large amounts of data. |
| **11.** | The goal of a known–plain text attack is to discover the encryption key. |
| **12.** | A cipher text–only attack attempts to crack the encryption using cryptoanalysis. |
| **13.** | Time and money are the two biggest concerns when attempting to break encryption using a brute-force method. |
| **14.** | WinMD5 can be used to verify the integrity of a file downloaded from the Internet. |
| **15.** | An x.509 certificate includes a field for Issuer and Public Key. |
| **16.** | x.509 is the standard for digital certificates. |
| **17.** | Different values such as 1 and 0 in an XOR process result in a value of 1. |
| **18.** | CA (certificate authorities) and digital certificates are two components of a PKI. |
| **19.** | Integrity ensures the data is not modified in transit. |
| **20.** | A hash is a one-way encryption used to validate the integrity of a file. |