**CSC 312 Cybersecurity**

|  |  |  |
| --- | --- | --- |
| **50 Points** | **CH07-08** | **Assignment 05** |

**Fill in the Blank (20 Points)**

1. **Cryptanalysis** - The process of attacking encryption by trying to recover information hidden in an encrypted message.
2. **Key stream** -The sequence of binary bits that encrypts the data stream in a stream cipher.
3. **Transposition cipher** - A cipher that rearranges the characters in the message's text.
4. **Substitution cipher** - A cipher that encrypts a message by substituting characters in the plaintext with different characters.
5. **DES** An obsolete US federal standard symmetric encryption algorithm; supported 56-bit keys.
6. **Asymmetric encryption** is a cryptographic algorithms that use different but related keys for encryption and decryption.
7. **Certificate Authority -** is a trusted third party that issues public key certificates to reliably identify the owner of a public.
8. **Session key -** is a key used to encrypt an arbitrarily large amount of static data, like a file.
9. **Key distribution center -** is the set of users or other entities that share a specific secret key.
10. **Digital signature -** is check value that is created using a private key and validated using the corresponding public key.
11. **Volatile key** - is a key constructed inside a process and procedure and never preserved outside that environment.
12. **Key encryption -** is a key used to encrypt other keys.
13. **Man-in-the-middle** - is an attack that intercepts all traffic between two endpoints and modifies it in transit.
14. **Private key -** is the key used in public-key cryptography that the owner must keep secret.
15. **Public key -** is the key used in public-key cryptography that is related to the private key and may be published.
16. **Key rollover -** is the process of replacing a key currently in use with a new key.
17. **Separation of duties** - is the principle of dividing a task among multiple entities so that no one can perform the task alone.
18. **Key wrapping -** is encrypting a shared key, usually with symmetric encryption.
19. **RSA -** is the first successful public-key algorithm, based on modular.

1. **Block Cipher** - is a cipher that encrypts and decrypts binary data in blocks of a fixed size.

**Multiple-choice questions: (10 points)**

1. An encryption algorithm that uses the same key for both encryption and decryption is:
2. symmetric
3. asymmetric
4. ciphertext
5. none of the above
6. The type of cipher that rearranges the text of a message is called:
7. substitution
8. asymmetric
9. AES
10. Transposition
11. File encryption on the computer’s hard drive involves what risk?
12. Access to low-level data written to the hard drive
13. Access by a Trojan Horse
14. Access by a separately booted OS
15. All of the Above
16. The encryption procedure requires two inputs:
17. ciphertext and plaintext
18. key and plaintext
19. key and a ciphertext
20. algorithm and key
21. The attack in which analyst can select plaintexts to be encrypted with the target’s secret key
22. Known plaintext
23. Chosen plaintext
24. Known ciphertext
25. Ciphertext-only
26. The following are common ways to handle new encryption keys *except*:
27. memorize them
28. write them down
29. save them to a storage device and download as needed
30. transfer them via instant messenger
31. Encrypting an encryption key using a passphrase is called:
32. asymmetric cryptography
33. key exchange
34. key wrapping
35. modular inversing
36. In a Diffie-Hellman calculation using *, s* is:
37. the unique public value computer from the private key
38. the private key value
39. a public, shared value
40. the modulus
41. You should rekey an encryption key:
42. when a key is leaked to unauthorized parties
43. when some major event occurs, such as a major new version of the file that the key protects
44. more often on larger cryptonets
45. All the above
46. A successful bit-flipping attack requires:
47. knowledge of the exact contents of the ciphertext
48. a stream cipher
49. knowledge of the exact contents of the plaintext
50. b and c

**True or False Questions (10 points):**

|  |  |  |
| --- | --- | --- |
| # | Statement | True or False |
| 1 | The two primary types of symmetric algorithms are public and cipher. | False |
| 2 | The Vigenère cipher uses a series of shifts to encrypt every letter in a message. | True |
| 3 | For encryption to work there must always be a matching decryption algorithm. | True |
| 4 | An encryption application program, from a user’s point of view, protects a file with a memorized password. | True |
| 5 | After changing an encryption key, all backup copies of the protected file are also protected by the new key. | True |
| 6 | The shorter the encryption key, the more difficult it is to crack. | False |
| 7 | An attacker can modify a file without changing the file’s hash value. | True |
| 8 | In cryptography, an internal key exists inside the encryption process and disappears when the process is not running. | True |
| 9 | When you visit a website with an “https” prefix in the address, the site is secure. | True |
| 10 | The Diffie-Hellman cipher is a full encryption method. | False |

**Essay Questions (10 points):**

1. Compare the advantages and disadvantages of memorizing a passphrase versus writing it down.

* No physical record of it to be lost or stolen
* Difficulty memorizing passwords that are long and complex
* Writing down passwords can help people remember their keys. This does create a vulnerability of someone stealing/finding your records.
* This can be prevented by storing them in safe place.

1. Briefly address the main difference between the stream cipher and block cipher.
2. Stream ciphers encrypt **bit by bit**
3. Block ciphers encrypt fixed-sized **blocks of bits**
   * The block cipher takes the block of data and encrypts it into an equal-sized block of data
   * For example:
     + DES worked with 64- bit blocks of data (Data Encryption Standard)
       - Search space: 256 (3)
     + AES works on 128-bit blocks (Advanced Encryption Standard)
       - Search space 2128 Better more secure than DES
       - three different keys in AES 128 129 and 256

* bit size of the key is not dependent on the bit size of the block!

1. Using a Caesar cipher that shifts letters three places, so that A becomes D, decode this phrase: **zhoo grqh**. == “well done"
2. Provide a brief explanation of the reused key stream problem in stream ciphers.

When the key stream is reused to encrypt multiple plaintexts, the attacker can use XOR to two cipher texts to get the XOR of two plain texts.

To counter this stream ciphers should have unique key streams (byway of an initialization vector)

1. Suppose that Bob and Alice have agreed on the Diffie-Hellman shared values to exchange a secret key as following:

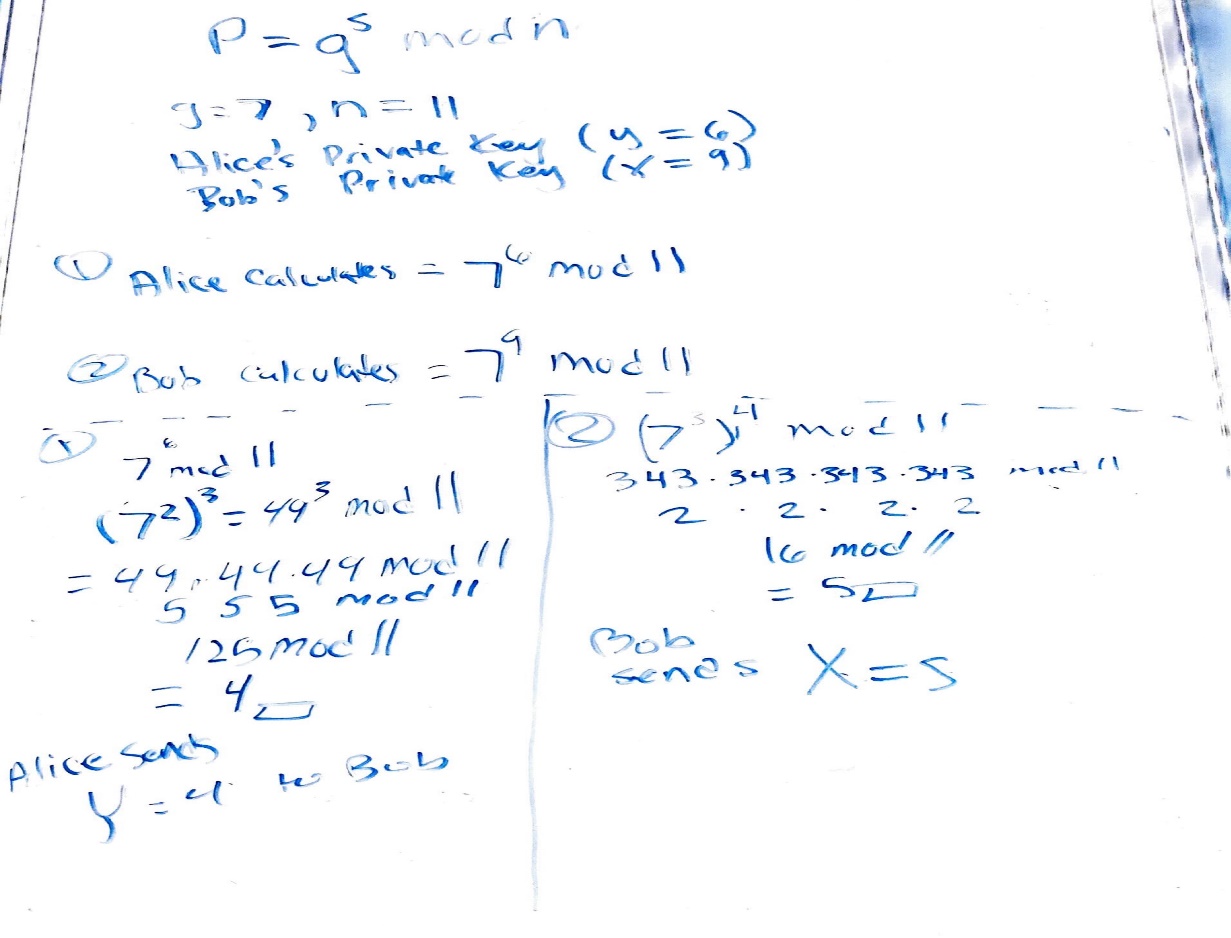
* G= 7, N= 11
* Alice’s private key y = 6
* Bob’s private key x = 9

Compute the intermediate values and the final key that Alice and Bob exchange.

*The Basic Math: D-H*

**P = gs mod N**

* p is the public key
* s is the private key randomly chose less than N
* g is a public shared value often g = 2
* N is a very large prime number
* G and N shared between users incredibly
* Discrete logarithm problem the log is the inverse of exponentiation but the prime modulus make the exponentiation hard to invert.
* Both participants must have a public and private key pair
* Each one multiplies their own private key by the other's public key to compute the shared secret



Correction bob sends x=8!!! Messed up on 2 but the next part is corrected.

