Problem Set 2

Michael Lee

Crypto concepts and classical ciphers

1. Concepts
    a. A cipher is an algorithm to encrypt messages so that they are unreadable without decryption.
    b. A transposition cipher rearranges the characters in the message while a substitution cipher substitutes the characters with other characters.
    c. Classify
        i. Rail Cipher – Transposition
        ii. Book Cipher – Substitution
2. Encrypt using Columnar Transposition
    a. PRUYRISPTSOTEIINLNACMECTPCEDCECUSRIIPARI

WORD
4 2 3 1
C O M P
U T E R
S E C U
R I T Y
…

3. OTP is a vigenere cipher that has proven to be unbreakable given the assumed conditions which requires a truly random key as long as the message
    a. CLESDPNYOTPYFQTYFASAEWJEEYIGINDMJDLPRJAH
4. a, b, c

Modern Symmetric Crypto

5. Stream ciphers are one to one in that they convert one text symbol directly to one cipher text, while block ciphers encrypt a group of text as one block.
    a. S
    b. S
    c. B

6. Stream ciphers are faster and more compact than a block cipher, and can encrypt messages of any length.

7. Block ciphers are more versatile than stream ciphers; for instance, block ciphers can be used as a foundation to build stream ciphers, hash functions, etc.

8. They differ by n/2 bits.

9. AES. AES is the successor to DES, and while 3DES improves upon DES, AES is faster and uses larger blocks of 128 bits.

10. DES is no longer considered secure because it uses a 56-64 bit key which is too short. It can be brute forced within a matter of days with current technology. 2DES doesn't give much added security as the attacker can both encrypt and decrypt to find out where they meet in the middle to break the encryption.

11. 56-bits * 3 makes 168 key independent bits, but as discussed above there is only 56 * 2 or 112 bits of security because of man in the middle attacks which make It weaker.

12. An encryption or cipher mode is the way block encryption can feed back on itself or not like in ecb, cbc or ofb. One disadvantage of using ECB mode is that each block is encrypted independently, and so identical blocks will create identical ciphers.

13. Picture problem
    a. Ci = Ek(m XOR Ci-1) for i > 0 and Mi = Dk(Ci) XOR Ci-1, if i=0 then the Initialization vector takes place of Ci-1.
    b. Cipher block chaining mode.
    c. Initialization vector should be different each time like a salt, otherwise it is essentially the same as ECB mode, and so you can't fix it ahead of time.
14. In counter mode you can generate bits in the middle of the stream so it lets you operate on blocks in parallel, and it doesn't need an initialization vector unlike OFB mode.

15. Yes, block ciphers can easily be converted into stream ciphers by simply setting the block size to a single character.

16. It should be efficient, one-way (you can't feasibly work backwards), and strong or weak collision resistance.

17. A birthday attack is where the attacker generates a large number of variations of valid messages and their desired fake message, and then by the birthday paradox the probability of finding a pair with the same hash is > 50%. It would take an attacker 2^32/2 or 2^16 until they have a 50% chance of success.

18. A cryptographic checksum is a hash that is used to check if data has been changed or corrupted, while a MAC combines a shared secret key with the message to authenticate and ensure that the message is correct or unaltered. MAC should be used if they want to ensure that the message is coming from the right person on an open channel.

Public key crypto and digital signatures

19. Secret key uses a single key to encrypt and decrypt messages while public key uses two. With public key encryption, one key (the public key) doesn't have to be kept secret and

the communication is still considered secure. Public key encryption can be used for confidentiality and authentication depending on which key, public or private, you use to encrypt the message.

20. Alice-Bob
    a. She should first encrypt here message with the public key assuming public key: (e,n) and message: m -> c = m^e mod n, then send c to bob.
    b. If this is the only message that Bob has received, then he should not send his credit card information over. In theory anyone could have sent that message there is no authentication. Instead Alice could encipher and authenticate using her private key and bob's public key, where private key: d and bob's public key: (e,n) -> c = (m^d mod n)^e. This would ensure that the message is encrypted and bob would know that Alice was the one who sent the message.
    c. Enciphering the message in blocks would allow Alice to encrypt her message much faster thereby minimizing the effort needed. In addition, the attacker couldn't alter letters to change message meaning leaving them more protected.

21. MAC algorithms are slower than digital signatures. Digital signatures are created by the private key (as talked about above), only the holder of the key can create the signature and therefore anyone, as the public key is public, can verify and decrypt it. MAC on the other hand protects a message from anyone who doesn't know the shared key between sender and receiver.

22. Man in the middle is an active attack where the hacker 'sits' in between two people intercepting their communications and relaying or falsifying messages. Meet in the middle is completely different in that it occurs offline and tries to brute force a problem, but significantly reduces the time complexity with space like the one used to break 2DES.

23. Hashing the message results in a much shorter value than the original message which saves time. Assuming the hash is unique then any change in the data would show that the message was corrupted or tampered with. While it is not necessary to hash the message, it makes it much faster and convenient.