Vincent Yasi

CS 370 -Intro to Security-

Problem Set 2

What is Crypto?

Q1 [6 pts]: Name the four cryptographic tools discussed in the "What is Crypto" lecture video and list the security properties that each of those tools support?

- Encryption/Ciphers: these support Confidentiality and Privacy by encrypting and keeping "hidden" messages and data
- Hashes: these support Integrity by helping to ensure the data sent/received is what was encrypted
- MACs: these support Integrity by insuring the message
- Digital Signatures: these support Integrity, Authenticity, and Non-Repudiation by verifying the source of the message in a secure way

What is Encryption?

Q2 [3 pts]: What is a cipher? What is it used for?

A cipher is a scheme or function used to encrypt and obfuscate a message or data in such a way to make it secure if it falls into the hands of an adversary, and done in such a way that the appropriate party can decrypt it.

Q3 [4 pts]: What is the difference between a symmetric cipher and an asymmetric cipher? What is one advantage of a symmetric cipher over asymmetric and vice-versa?

A symmetric cipher involves using the same key for the encryption and decryption of the plaintext/ciphertext.

An asymmetric cipher involves different (though often related) keys for the encryption and decryption.

An advantage of a symmetric cipher is that it is usually easier to use than asymmetric as it only involves one key and can often use simpler encryption schemes. The key is also typically easier to generate as you do not need to deal with things like using RSA functions to generate compatible keys.

An advantage of asymmetric ciphers over symmetric is that asymmetric is often more secure, as plaintext can be encrypted with a public key without any knowledge of the private key used to decrypt it, and a "leak" of the encryption key (which cannot really be leaked, as it is public already) does not allow one to decode to message.

Q4 [3 pts]: What is a brute force attack on a cipher? Explain it using "known plaintext" adversary and "ciphertext only" adversary.

A brute force attack is trying to calculate all possible forms/values for information you do not know (such as the key) so as to break the encryption.

In known plaintext, it would be trying to calculate all possible keys which could be used to encrypt the known plaintext to get the known ciphertext until you find the one which was used.

In ciphertext only, it would be also trying to generate all possible keys until one, when used to decrypt the ciphertext, gives a comprehensible plaintext and seemingly the original one.

Q5 [3 pts]: How may an adversary improve over a brute force attack?

There are many ways to improve over a brute force attack. Most all involve trying to deduce some advantage or similar piece of knowledge which can be used to decrease the amount of work needed to calculate what you want or to derive some information about the plaintext (or whatever information you are looking for). This can be things like looking for patterns between multiple ciphertexts generated by the same algorithm to gain knowledge of similarities in plaintext and how the function encrypts, sending specific messages through encryption (if able to) to analyze the ciphertext, and trying solutions using certain common letters or words.

Classical Ciphers

Q6 [2 pts]: What is the difference between a substitution cipher and transposition cipher?

A substitution cipher substitutes one letter (or piece of data) for another in a particular way, such as all A's are now E's.

A transposition cipher shifts (or transposes) letters and data in a certain way based on a key, such as shifting each letter down three places in the alphabet.

Q7 [4 pts]: What is a one-time pad? Why is the book cipher not as secure as one-time pad?

A one-time pad uses a one-time use, random key of the same length as the data to be encrypted, and performs some operation (such as modulo addition or XORing) between the key and plaintext. The result is the ciphertext.

A book cipher is not a secure one-time pad because it uses sequential text from a book as the key in the encryption. However, this key is not random, as it is English (or some other) language, and so has patterns, etc. Therefore, even without knowing which book/block of text was used to encrypt, information can be gleaned by analysis.

Modern Ciphers

Q8 [3 pts]: What the difference between a stream cipher and a block cipher?

A stream cipher encrypts with a key which is broken into pieces, and each piece used in an encryption step as its own key. The key typically has to be at least as big as the plaintext.

A block cipher instead breaks the plaintext into blocks used in each encryption step, but the key generally stays the same for each step. This also means the key can be smaller than the plaintext, and is often the size of a block.

Q9 [2 pts]: What is the advantage of a stream cipher over a block cipher?

A stream cipher has a constantly changing key (as a different value is used at each step), and so it is harder to decrypt or figure out the whole key.

Q10 [2 pts]: What is the advantage of a block cipher over a stream cipher?

A block cipher can be performed with a key smaller than the plaintext, and through the use of padding, can even encrypt plaintexts of variable lengths.

Q11 [2pts]: A good block cipher exhibits avalanche effect: if we flip one bit in the plain text, half of the bits are flipped in the cipher text. Two messages of the same length, m1 and m2, differ by 5 bits. With a good block cipher, how many bits differ in the two resulting cipher texts? Assume both cipher texts are n bits long.

About 96% of the ciphertexts should differ. For each bit the plaintexts differ, about half of the bits will be flipped. If this happens in 5 places/at 5 bits, this would mean about 96% of the bits would differ (0.5*0.5*0.5*0.5*0.5).

Q12 [3pts]: If you are starting a new project that does not depend on other legacy programs, which cipher would you use, 3DES or AES? Justify your answer.

I would use AES. It is the current standard and offers greater security than 3DES. It also protects better against common modern attacks.

Q13 [4pts]: Why is DES no longer considered secure? Can we use Double DES (2DES) instead? Why or why not?

DES (and also 2DES) can rather easily be broken with Meet-In-The-Middle attacks using modern technology. Even running the encryption twice (2DES) does not give adequate protection with modern resources.

Also, the basis from which DES and 2DES were built is not public, and therefore does not have much transparency. This leads to issues, especially against the open AES scheme.

Q14 [4pts]: What is the bit strength of 3-DES when used in Encrypt-Encrypt-Encrypt mode? Explain Why. (Assume the keys are independent)

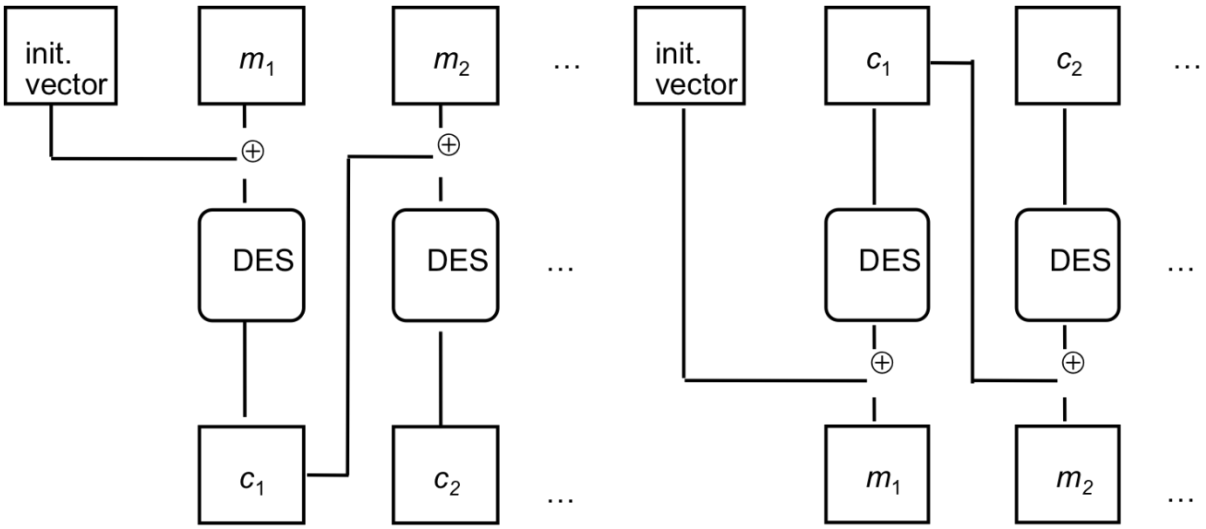
The bit strength is the same as the base DES: 56 bits. This is because, even though the scheme encrypts three times, and uses a total of 168 bits, each encryption can be broken with an MTM attack. The first encryption can be broken by meeting between the first encryption and the two other encryptions, and then as a second step, doing the same between the second and third encryptions. Therefore, the total bit strength is only the size of one encryption key, which is 56 bits. It is essentially performing the MTM attack for normal DES, just doing it twice, instead of once.

Encryption Modes

Q15 [3pts]: What is an encryption mode or cipher mode? Name one disadvantage of using ECB mode.

An encryption mode is a way that block ciphers can encrypt messages larger than a single block size, often with multiple cycles.

ECB mode is generally pretty bad because it directly encrypts each block of the plaintext (as opposed to modifying it based on the other blocks or some other principle). Therefore, same blocks in the plaintext will always encrypt to the same block of ciphertext. This can be used to reverse the ciphertext, as well as allow for cutting and pasting of the ciphertext directly to change the plaintext message.



Q16 [10pts]: The above picture represents encryption and decryption modes for a block cipher (here DES).

a) [4 pts] Complete the equations that describe the above encryption and decryption operations.

$$\boldsymbol{ENC}: c_i = DES(m_i \oplus c_{i-1}); c_0 = IV$$
$$\boldsymbol{DEC}: m_i = DES(c_i) \oplus c_{i-1};\ c_0 = IV$$

b) [2 pts] What is this mode called?

This is CBC mode.

c) [4 pts] What properties should the initialization vector (IV) have? Can one fix the initialization vector ahead of time? Why or why not?

The IV should be one block length and at least pseudo-random. The IV can be fixed ahead of time. As it is not dependent upon the plaintext (or ciphertext), as long as it is appropriately random, it does not matter if it is prepared ahead of time, as long as it is secret. If it is not secret, then information can be derived about the plaintext, as one knows the first block is XORed with the IV before it is run through the DES algorithm

Q17 [3pts]: What are the advantages of Counter mode over OFB mode?

With OFB mode, the key each cycle is generated by running the previous key through the encryption algorithm to get the new key. This creates an overall final key that is multiple block lengths.

With Counter mode, the key is incremented each time before encryption, as opposed to based on the previous iterations. Therefore, the key just needs to be one block length (for the first cycle), and the incrementation used for the counter. This allows for a much smaller overall key (and therefore less storage and data space, and less risk of bit errors).

Q18 [3pts]: Is it feasible to convert a block cipher into a stream cipher? If yes, give an example.

For certain block ciphers, it is feasible, such as with OFB mode. Generally, if a block cipher uses a block length key in each cycle, this key can be replaced with one block of a stream cipher-type key.

For example, for OFB, in its block cipher form it takes in an IV and runs it through an algorithm each cycle to get the key used for that cycle. Instead of running the previous key through the algorithm each cycle to get the new key, it could instead use the next block of the stream key and skip the algorithm. This would create a rather weak encryption scheme without further modifications, as then each cycle the key and plaintext block would only be XORed together to get the ciphertext block, but it would still function.