CS361 Questions: Week 3

The questions marked with a dagger (†) require external research and may be more extensive and time consuming. You don't have to do them for the assignment but, but do them to increase your competency in the class.

Lecture 34

1. Why is it impossible to transmit a signal over a channel at an average rate greater than C/h?

   If a channel has capacity C, that means C is the maximum bits/second able to be sent through that channel. That number doesn't change. If a message/language/source has entropy h, that won't change either. So the total number of signals able to be sent is the Capacity (bits/second of channel) divided by h (entropy – bits/signal) which gives signals/second.

2. How can increasing the redundancy of the coding scheme increase the reliability of transmitting a message over a noisy channel?

   It means that if you send a message and part of it is muddled by noise, sending it again gives a higher chance to clarify the part distorted by the noisy channel.

Lecture 35

1. If we want to transmit a sequence of the digits 0-9. According to the zero-order model, what is the entropy of the language?

   $H = -(\log 1/10) = 3.322$

2. What are reasons why computing the entropy of a natural language is difficult?

   Because there are many ways to send a message and have the same idea come across: Ex: Cambridge research message.

3. Explain the difference between zero, first, second and third-order models.

   Zero: all letters are equally likely at any point in the message/word, etc.
   First: all symbols are independent of each other but they aren't equally likely.
   Second: estimates likelihood of pairs of letters; not equally likely.
   Third: computes likelihood of trigrams.

Lecture 36

1. Why are prior probabilities sometimes impossible to compute?

   Because it's hard to compute the level of knowledge after information has been learned

2. Why is the information content of a message relative to the state of knowledge of an observer?

   Because if the observer knows more of the subject, less information needs to be sent

3. Explain the relationship between entropy and redundancy.

   If there is higher redundancy, the entropy will be lower and the encoding easier.

Lecture 37

1. List your observations along with their relevance to cryptography about Captain Kidd's encrypted message.

   Message contains numbers and symbols. Certain sequences are repeated. Certain numbers/symbols are used more than others. If it's captain Kidd's, it will likely be a simple encryption because he's a pirate. We don't know language we're decrypting.

2. Explain why a key may be optional for the processes of encryption or decryption.

   If the encryption is very basic, perhaps the "key" will be obvious enough or perhaps the encryption can be done by an algorithm without a key.

3. What effect does encrypting a file have on its information content?

   It hides the plaintext message, but also preserve it so the receiver can extract the message.

4. How can redundancy in the source give clues to the decoding process?

   The redundancy could give clues to a pattern, which could help decode the message by an attacker.

Lecture 38

1. Rewrite the following in its simplest form: D(E(D(E(P)))).

   1 Encrypt plaintext, 2 decrypt, 3 encrypt, 4 decrypt.

2. Rewrite the following in its simplest form: D(E(E(P,KE),KE),KD).

   Encrypt P with KE, encrypt that with KE, Decrypt that with KD.

3. Why might a cryptanalyst want to recognize patterns in encrypted messages?

   Traffic analysis, which gives the analyst some information about the context/meaning without breaking the algorithm.

4. How might properties of language be of use to a cryptanalyst?

   Could give hints to the meaning of certain letters/words based on placement in sentence or word.

Lecture 39

1. Explain why an encryption algorithm, while breakable, may not be feasible to break?

   It could take a very, very long time to get the correct answer, or the subject may not be able to determine if the cipher gave you the write answer.

2. Why, given a small number of plaintext/cipher text pairs encrypted under key K, can K be recovered by exhaustive search in an expected time on the order of 2n−1 operations?

   Because that gives every possible value for the key in those 2n-1 operations.

3. Explain why substitution and transposition are both important in ciphers.

   Substitution switches the symbols for another symbol and transposition moves the symbols around. Together, the encryption is much stronger

4. Explain the difference between confusion and diffusion.

   Confusion transforms the information so an interceptor won't be good at reading it (substitution is good at this) while diffusion spreads the information widely over the ciphertext (transposition is good at this).

5. Is confusion or diffusion better for encryption?

   Alone, neither is better. Together they are best.

Lecture 40

1. What is the difference between monoalphabetic and polyalphabetic substitution?

   Monoalphabetic is uniform. Every occurrence of x is replaced by y. Polyalphabetic has different letters substituted based on where the character occurs in the plaintext.

2. What is the key in a simple substitution cipher?

   A table or diagram showing which character represents another.

3. Why are there k! mappings from plaintext to ciphertext alphabets in simple substitution?

   Because the mappings are uniform and contain k characters.

4. What is the key in the Caesar Cipher example?

   However many letters are shifted to get cipher.

5. What is the size of the keyspace in the Caesar Cipher example?

   25

6. Is the Caesar Cipher algorithm strong?

   No.

7. What is the corresponding decryption algorithm to the Vigenere ciphertext example?

   Monit orsto gotot hebat hroom is the key and is used with a vigenere tableau.

Lecture 41

1. Why are there 17576 possible decryptions for the "xyy" encoding on slide 3?

   26*26*26 = 17576

2. Why is the search space for question 2 on slide 3 reduced by a factor of 27?

   Because x &y must be different, and both the y's must be the same.

3. Do you think a perfect cipher is possible? Why or why not?

   No, because every cipher can be broken by brute force eventually.

Lecture 42

1. Explain why the one-time pad offers perfect encryption.

   Every possible plaintext oculd be the pre-image of that ciphertext under a plausible key. So no reduction of the search space is possible.

2. Why is it important that the key in a one-time pad be random?

Because then you can work backwards and eliminate some of the plaintexts, so it's no longer perfect.

3. Explain the key distribution problem.

If the sender and receiver already have a secure channel, why do they need the key? Also, if they don't how do they distribute the key securely?

Lecture 43

1. What is a downside to using encryption by transposition?

The original characters of the plaintext still occur in the ciphertext.

Lecture 44

1. Is a one-time pad a symmetric or asymmetric algorithm?

   Symmetric

2. Describe the difference between key distribution and key management.

   Key distribution is about sharing a key secretly, while key management is about keeping the keys safe when storing them.

3. If someone gets ahold of Ks, can he or she decrypt S's encrypted messages? Why or why not?

   No, because decryption is done with S's private key.

4. Are symmetric encryption systems or public key systems better?

   They solve the problem of getting a key to someone securely.

Lecture 45

1. Why do you suppose most modern symmetric encryption algorithms are block ciphers?

   Because I/O operations are expensive and slow

2. What is the significance of malleability?

   if you can change the ciphertext and produce meaningful changes in the plaintext, it's easier to completely change the plaintext.

3. What is the significance of homomorphic encryption?

Allows the ability to perform changes on ciphertext that when decrypted show up in the plaintext.

Lecture 46

1. Which of the 4 steps in AES uses confusion and how is it done?

subBytes, addRoundKey

2. Which of the 4 steps in AES uses diffusion and how is it done?

mixColumns, shiftRows

3. Why does decryption in AES take longer than encryption?

Everything is done in reversed order. InverseMixColumns has different multiplication values that are harder to optimized.

4. Describe the use of blocks and rounds in AES.

Arranges block into 4x4 bytes called a state, go through rounds of operations combining confusion and diffusion.

5. Why would one want to increase the total number of Rounds in AES?

Make the algorithm more secure and difficult to break.

Lecture 47

1. What is a disadvantage in using ECB mode?

   Identical blocks in plaintext result in identical ciphertext blocks.

2. How can this flaw be fixed?

   Randomize plaintext blocks before they're encrypted (Cipher block Chaining)

3. What are potential weaknesses of CBC?

   Attacker can observe and spot the first block that is changed. If he finds two identical ciphertext blocks, he can derive a relation.

4. How is key stream generation different from standard block encryption modes?

   Cipher used as pseudorandom number generator so the output appears random but is reproducible.

Lecture 48

1. For public key systems, what must be kept secret in order to ensure secrecy?

Private keys which is used for decryption

2. Why are one-way functions critical to public key systems?

easy to compute but difficult to inverse: multiplication. These are critical because encryption should be easy while decryption shouldn't.

3. How do public key systems largely solve the key distribution problem?

it solves the problem of a secret encryption key.

4. Simplify the following according to RSA rules: {{{P}K−1}K}K−1.

{P}K-1

5. Compare the efficiency of asymmetric algorithms and symmetric algorithms.

Symmetric algorithms are much more efficient (as much as 10000 times) than asymmetric.

Lecture 49

1. If one generated new RSA keys and switched the public and private keys, would the algorithm still work? Why or why not?

   Yes, because they work in a symmetric way.

2. Explain the role of prime numbers in RSA.

   The keys are based on factoring large numbers.

3. Is RSA breakable?

   Yes

4. Why can no one intercepting {M}Ka read the message?

   No, because they don't have the private key

5. Why can't A be sure {M}Ka came from B?

   Anyone might have A's public Key.

6. Why is A sure {M}K−1 originated with B?

Because only B has his private key

7. How can someone intercepting {M}K−1 read the message?

   By using the public key.

8. How can B ensure authentication as well as confidentiality when sending a message to A?

   By using 2 different types of keys.

Lecture 50

1. Why is it necessary for a hash function to be easy to compute for any given data?

2. What is the key difference between strong and weak collision resistance of a hash function.

   Strong collision resistance prevents collisions even when the messages are the same. Weak collision resistence prevents collisions when the messages are different.

3. What is the difference between preimage resistance and second preimage resistance?

   Preimage resistant if given a hash its hard to find the message that hashes to that value. Second preimage resistance prevents the same hash value when the messages are different.

4. What are the implications of the birthday attack on a 128 bit hash value?

   On average, have to look at 1.25*2^64 before you find a collision.

5. What are the implications of the birthday attack on a 160 bit hash value?

   On average, have to look at 1.25*2^80 before you find a collision.

6. Why aren't cryptographic hash functions used for confidentiality?

   They're more concerned with who sees the hash value.

7. What attribute of cryptographic hash functions ensures that message M is bound to H(M), and therefore tamper-resistant?

   Strong collision resistance

8. Using RSA and a cryptographic hash function, how can B securely send a message to A and guarantee both confidentiality and integrity?

   Use the hash function then encrypt with public key, then decrypt with private key.

Lecture 51

1. For key exchange, if S wants to send key K to R, can S send the following message: {{K}KS−1}K−1? Why or why not?

   Yes, but it is decryptable by the public keys

2. In the third attempt at key exchange on slide 5, could S have done the encryptions in the other order? Why or why not?

   No, because then you wouldn't know who it was coming from, and the receiver couldn't decrypt it.

3. Is {{{K}KS−1}KR}KS equivalent to {{K}K−1}KR?

   Yes

4. What are the requirements of key exchange and why?

   Both authentication and confidentiality.

Lecture 52

1. What would happen if g, p and gamodp were known by an eavesdropper listening in on a Diffie-Hellman exchange?

   They cant decrypt the message because they don't know a &b.

2. What would happen if a were discovered by an eavesdropper listening in on a Diffie-Hellman exchange?

   They can't decrypt the message

3. What would happen if b were discovered by an eavesdropper listening in on a Diffie-Hellman exchange?

They can’t decrypt the message