Name: Tyler Kemme
UTEID: tpk266
CS ID: tpkemme
Email: tpkemme@gmail.com

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?

It is impossible to transmit faster than C/h because the channel cannot transmit faster than its rate, C. Also, to get better than C/h, you would have to have a perfect encoding of the language.

2. How can increasing the redundancy of the coding scheme increase the reli-

ability of transmitting a message over a noisy channel?

If you increase the redundancy, then no matter how much noise is present in the channel, your message will eventually make it through.

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?

The entropy according to the zero-order model of the sequence is 1.

2. What are reasons why computing the entropy of a natural language is diffi-

cult?

It is difficult to compute the entropy of a natural language because it's very difficult to compute the probability of a word occurring in a language.

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

The zero order model assumes that the probability of all words in a language are equal. The first order model assumes that each word occurs a specific number of times but that the probability of a word occurring is independent of all other words. The second order model says that the probability of a word in a language is dependent on the word that just occurred. The third model says that the probability of a word occurring in a language is dependent on the last two words.

Lecture 36

1. Why are prior probabilities sometimes impossible to compute?

Sometimes it's hard to compute prior probabilities because sometimes the probability of an event occurring is different depending on the knowledge of the subject.

2. Why is the information content of a message relative to the state of knowl-

edge of an observer?

Information content of a message is relative to the state of knowledge of the observer because a message might have very important information but if the object has no knowledge of the context of the message than the data is worthless.

3. Explain the relationship between entropy and redundancy.

Generally, if the information content of a language is the same length as the encoded message, then there is no redundancy.

Lecture 37

1. List your observations along with their relevance to cryptography about

Captain Kidd's encrypted message.

Captain Kidd's encrypted message is important because it presents the problem of how to decrypt an encrypted message without knowing the language of the plaintext, the complexity of the encryption algorithm, and other properties relating to the process of transforming the plaintext to an encrypted message.

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

cryption.

An encryption algorithm only needs a key value when each encryption has to be different depending on the k. If there isn't a key, the encryption of the same message would produce the same output.

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

The encryption of information content needs to *hide* the content of a message without distorting the original information.

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

Redundancy gives clues because it shows that the encryption algorithm produces the same results for all input which makes it much easier to decrypt.

CS361 Questions: Week 3 2

Lecture 38

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

P

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

{{{P}KE}KD}KE

3. Why might a cryptanalyst want to recognize patterns in encrypted mes-

sages?

If you recognize a pattern in the encrypted language, that could be used to infer information about the original message or the encryption algorithm.

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

If the cryptanalyst knows properties of the language, it may be easier to find similar patterns in the encrypted message.

Lecture 39

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

to break?

It may be possible to test every possible key/plaintext combination but that could take an arbitrarily large amount of time.

2. Why, given a small number of plaintext/ciphertext pairs encrypted under

key K, can K be recovered by exhaustive search in an expected time on the

order of 2 n − 1

operations?

K can be recovered in 2^n-1 operations because assuming K has n bits, there are 2^n-1 possible bit combinations that K could be.

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

Substitution is important because it keeps symbols from being the same in the plaintext and the cipher text. Transposition is important because it keeps the original sequence of symbols from showing up in the cipher text. The combination of the two operations makes the cipher text unrecognizable from the plaintext.

4. Explain the difference between confusion and diffusion.

The difference between confusion and diffusion is similar to the difference between substitution and transposition. Confusion makes sure that information is transformed so that it's hard to get the original information. Diffusion means that information is spread over different parts of the cipher text so that the cipher text does not have the same flow of information as the plaintext.

5. Is confusion or diffusion better for encryption?

Confusion is generally better for encryption but both confusion and diffusion are necessary for a strong cryptosystem.

Lecture 40

1. What is the difference between monoalphabetic and polyalphabetic substi-

tution?

A polyalphabetic substitution is the same as a monoalphabetic substitution system except that symbols are transformed based on where they occur.

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

The key is a mapping between plaintext symbols and cipher text symbols.

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

substitution?

Since there is a 1-1 mapping between plaintext symbols and cipher text symbols, there are K! mappings in a language with K symbols.

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

The key in the Caesar Cipher is the amount of symbols you skip from the plaintext symbol to the cipher text symbol.

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

If there are 26 letters, then the keyspace is 26

6. Is the Caesar Cipher algorithm strong?

The algorithm is not strong because you don't have to brute force the cryptosystem to get the mappings.

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

example?

To decode the ciphertext, you find what letter maps to the ciphertext symbol based on the specific key.

CS361 Questions: Week 3 3

Lecture 41

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

3?

Because each letter has 26 possible letter choices and each letter is independent of each other.

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

Because each letter maps to only one symbol, then you know that x and y are going to map to different letters. There are 26 possibilities for the letter x, but once that mapping is found, there is one less mapping for y. Thus there are 650 possibilities.

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

I think a perfect cipher is not possible because it wouldn't be possible for someone to know the encryption algorithm and the ciphertext without being able to brute force the plaintext into cipher text.

Lecture 42

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

The one-time pad is perfect encryption because the ciphertext could be produced by literally any plaintext message of the same size.

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

If the key isn't random, then eventually the attacker could find a pattern in the key creation.

3. Explain the key distribution problem.

The problem with key distribution is finding a way to get the sender and the receiver the same key without any other users discovering the key.

Lecture 43

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

The downside of using encryption by transposition is that symbols don't change so the letter frequencies are preserved.

Lecture 44

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

One-time pad is symmetric because it uses the same key both times.

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

Key distribution involves getting the key to sender and receiver without letting other users see it. Key management involves securely storing all of these keys for each user.

3. If someone gets a hold of Ks, can he or she decrypt S's encrypted messages?

Why or why not?

No, Ks can only encrypt a message because it is the public key.

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

Public key systems are better because they use significantly less keys to communicate.

Lecture 45

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

block ciphers?

2. What is the significance of malleability?

Malleability is important because if the attacker can cause changes in the cipher text that produce meaningful results in the plaintext, the attacker can change the information in a message without decrypting it first.

CS361 Questions: Week 3 4

Lecture 46

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

subBytes uses confusion by using the value of the byte as an index into a substitution lookup table. mixColumns uses confusion by multiplying each column by a 4x4 array. addRoundKey also uses confusion by XORing the block with a key derived from the original key.

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

shiftRow uses diffusion by shifting bytes in each row.

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

Decryption takes longer because inverting the matrix when doing the opposite of mixColumns takes longer because it has larger numbers.

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

The blocks are same sized 2D arrays that hold the information as its converted from plaintext to ciphertext. The four steps of AES are repeated multiply times and each time is called a round.

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

The more rounds you use, the larger the key and the harder it is to brute-force discover the key.

Lecture 47

1. What is a disadvantage in using ECB mode?

The problem is that if blocks in the plaintext are the same, the ciphertext blocks will also be the same.

2. How can this flaw be fixed?

This way to fix this problem is to make sure that identical blocks in the plaintext are different in the ciphertext.

3. What are potential weaknesses of CBC?

Content Leak: If the attacker finds two identical ciphertext blocks then he/she can XOR them together to find information about the plaintext block.

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

modes?

The difference between key stream and block encryption is that in key stream generation the ciphertext is basically used as a pseudorandom number generator in the encryption of the plaintext.

Lecture 48

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

The private key must be kept secret.

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

If functions aren't one-way then it would be easy to invert these functions to get the plaintext.

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

The only key that needs to be shared (and the only key that an attack can see) is the public key. However, without the private key, the message is still secure.

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.

Asymmetric algorithms take much longer to compute because the operations are very complex.

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 it would because the keys always do the opposite of each other.

2. Explain the role of prime numbers in RSA.

A sequence of prime numbers don't follow any distinguishable pattern.

3. Is RSA breakable?

Yes but it would take an arbitrarily large amount of time to crack it.

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

Because only B has the Kb key.

CS361 Questions: Week 3 5

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

Because everyone has the public key Ka.

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

Because only B would have his private key K-1b.

7. How can someone intercepting {M} K − 1

b

read the message?

8. How can B ensure authentication as well as confidentiality when sending a

message to A?

By using one key system for privacy and one key system authenticity.

Lecture 50

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

data?

Because it has to be computed many times.

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

a hash function.

Strong collision means that collisions are impossible to find. Weak collision means that they are hard to find but not impossible.

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

resistance?

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

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

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

7. What attribute of cryptographic hash functions ensures that message M is

bound to H(M), and therefore tamper-resistant?

8. Using RSA and a cryptographic hash function, how can B securely send a

message to A and guarantee both confidentiality and integrity?

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

R

? Why or why not?

2. In the third attempt at key exchange on slide 5, could S have done the en-

cryptions in the other order? Why or why not?

3. Is {{{K} KS − 1 } K

R } K

S equivalent to {{K} K − 1

S

} K

R ?

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

CS361 Questions: Week 3 6

Lecture 52

1. What would happen if g, p and g

a

modp were known by an eavesdropper

listening in on a Diffie-Hellman exchange?

2. What would happen if a were discovered by an eavesdropper listening in on

a Diffie-Hellman exchange?

3. What would happen if b were discovered by an eavesdropper listening in on

a Diffie-Hellman exchange?