Mingu Chang(mc35926)

# 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 language has entropy h (bits per symbol) and a channel can transmit C bits per second, then it is possible to encode the signal is such a way as to transmit at an average rate of (C/h) − 2 symbols per second, where 2 can be made arbitrarily small. It is impossible to transmit at an average rate greater than C/h.

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

 For example, covert channels in the system cannot be dismissed with the argument that they are noisy and hence useless. You can always get the message through by finding a more redundant encoding.

## 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) = 1.00

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

 Computing the entropy of a natural language is difficult and requires complex models. The standard encoding for English contains a lot of redundancy. Spammers count on the ability of humans to decipher such text, and the inability of computers to do so to defeat anti-spam filters.

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

 Zero-Order Model: we assume all characters are equally likely; use log equation.
 First-Order Model: assume all symbols are independent of one another, but follow the specific probabilities, follow entropy 4.219 bits per symbol
 Second-Order Model: Adding diagrams to the computation.
 Third-Order Model: adding trigrams gives a third-order. 2.77 bits per symbol.

## Lecture 36

1. Why are prior probabilities sometimes impossible to compute?

 because we have several choices that we have to consider.

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

 Information content of a message depends on the state of knowledge of the receiver. Hence, entropy is relative to a particular observer.

3. Explain the relationship between entropy and redundancy.

Note that entropy can be used to measure the amount of “redundancy” in the encoding. If the information content of a message is equal to the length of the encoded message, there is no redundancy.

# Lecture 37

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

 goat's head, South Carolina beach, underlying language of the plaintext, characteristics of the probable source text,

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

 keys are often the same. Encryption and decryption process are same, just the opposite.

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

 Encryption is designed to obscure the meaning of text.

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

 Redundancy is the enemy of secure encryption because it provides leverage to the attacker.

# Lecture 38

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

 P P

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

 $D(E(C, K_E), K_D)$.

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

 to break a single message; to infer some meaning without breaking the algorithm; to deduce the key; to find weaknesses in the implementation or environment or
the use of encryption; to find weaknesses in the algorithm, without necessarily having intercepted any messages.

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

 The analyst works with properties of langauages

# Lecture 39

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

 The analyst must be able to recognize success. For that reason, having plaintext/ciphertext pairs available is often required. The longer the key, more impossible to break.

2. Why, given a small number of plaintext/ciphertext pairs encrypted under key K, can K be recovered by exhausteive search in an expected time on the order of $2^{N-1}$ operations?

 As N gets bigger, the search gets bigger.

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

 all modern commercial symmetric ciphers use some combination of substitution and transposition for encryption.

4. Explain the difference between confusion and diffusion.

 Substitution tends to be good at confusion; transposition tends to be good at diffusion.

5. Is confusion or diffusion better for encryption?

 We use both for encryption.

# Lecture 40

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

 A substitution cipher is one in which each symbol of the plaintext is exchanged for another symbol. If this is done uniformly this is called a

monoalphabetic cipher. If different substitutions are made depending on where in the plaintext the symbol occurs, this is called a polyalphabetic substitution.

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

 however you specify the mapping. (eg: table,etc)

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

 Redundancies in the plaintext are reflected in the ciphertext.

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

 how many positions you shift

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

 25 or 26 depending on how you look at it.

6. Is the Caesar Cipher algorithm strong?

 No probably not.

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

 fours scores seven years ago, monitors to go to the bathroom;
 Align the two texts, possibly removing spaces and then use the letter pairs to look up an encryption in a table.

# Lecture 41

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

 26^3 = 17576

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

 26 × 25 = 650.

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

 No probably not. There is no perfect cipher.

# Lecture 42

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

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

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

 you could take the ciphertext and that fact eliminates half the possible plaintext. This will make no long be a perfect cipher.

3. Explain the key distribution problem.

 If sender and receiver already have a secure channel, why do they need the key?

If they don’t, how do they distribute the key securely?

# Lecture 43

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

 Since transposition reorders characters, but doesn’t replace them, the original characters still occur in the result. Letter frequencies are preserved in the ciphertext, but the frequencies of digrams, trigrams, etc. are not.

# Lecture 44

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

 symmetric alorithm

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

For key distribution: how do we convey keys to those who need them to establish secure communication.

For key management: given a large number of keys, how do we preserve their safety and make them available as needed.

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

 Yes. Anyone wishing to send a message M confidentially to S sends

{M}Ks . Only the holder of (K^-1)s can decrypt this message.

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

 Symmetric encryption systems are better

# Lecture 45

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

 Most modern symmetric encryption algorithms are block ciphers. Block sizes vary (64 bits for DES, 128 bits for AES, etc.).
Because of high diffusion and immunity to tampering

2. What is the significance of malleability?

 Malleability means being able to manipulate ciphertext with predictable effects on plaintext.

3. What is the significance of homomorphic encryption?

    Homomorphic encryption is a form of encryption which allows specific types of computations to be carried out on ciphertext and generate an encrypted result which, when decrypted, matches the result of operations performed on the plaintext.

# Lecture 46

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

 subBytes: for each byte in the array, use its value as an index into a 256-element lookup table, and replace byte by the value stored at that location in the table.
shiftRows: Let Ri denote the i th row in state. Shift R0 in the state left 0 bytes (i.e., no change); shift R1 left 1 byte; shift R2 left 2 bytes; shift R3 left 3 bytes.
mixColumns: for each column of the state, replace the column by its value multiplied by a fixed 4×4 matrix of integers
addRoundKey: XOR the state with a 128-bit round key derived from the original key K by a recursive process.

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

 The decryption algorithm is the inverse of encryption, with the following differences: The subkeys are used in reverse order, Each of the steps is inverted, The first and last rounds are slightly different (Inverting the MixColumns step requires multiplying each column by the following fixed array).

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

 Because of the following from above #2 answers. (please look at #2 answers)

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

 AES uses a block of 128-bits. AES allows keys of size 128-bits, 192-bits, and 256-bits, with 10, 12, 14 rounds, respectively.

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

 

# Lecture 47

1. What is a disadvantage in using ECB mode?

 A naive use of encryption as in Electronic Code Book leaves too much regularity in the ciphertext.

2. How can this flaw be fixed?

 To solve the problem of EBC, do something to “randomize” blocks before they’re encrypted.

3. What are potential weaknesses of CBC?

 Observed changes: An attacker able to observe changes to ciphertext over time will be able to spot the first block that changed.
Content Leak.

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

 Block encryption modes (like ECB and CBC) generate ciphertext that stores the message in encrypted but recoverable form.

In key stream generation modes the cipher is used more as a pseudorandom number generator. The result is a key stream that can be used as in one-time pad. Decryption uses the same key stream.

# Lecture 48

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

 The basis of any public key system is the identification of a one-way function: easily computed, but difficult to invert without additional information.

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

 easily computed, but difficult to invert without additional information.

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

 A public key encryption may take 10,000 times as long to perform as a symmetric encryption; the computation depends on more complex operations, not on simple bit-wise operations.

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 encryption remains the work horse of commercial cryptography, with asymmetric encryption playing some important special functions. Asymmetric algorithms are generally much less efficient than symmetric algorithms.

# 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?

2. Explain the role of prime numbers in RSA.

RSA is the most widely used public key cryptosystem. RSA is symmetric in the use of keys; most public key schemes are not.

3. Is RSA breakable?

4. Why can no one intercepting $\{M\}_{K_A}$ read the message?

 No-one intercepting the message could read it. He can't be sure it actually came from B.

5. Why can't A be sure $\{M\}_{K_A}$ came from B?

6. Why is A sure $\{M\}_{K_{B^{-1}}}$ originated with B?

7. How can someone intercepting $\{M\}_{K_{B^{-1}}}$ read the message?

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

# Lecture 50

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

A cryptographic hash function has the additional qualities:
it is difficult to construct a text that has a given hash,
it is difficult to modify a given text without changing its hash,
it is unlikely that two different messages will have the same
hash.

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

A function f is second preimage resistant if, given an input m1, it is hard to find m2 6= m1 such that f (m1) = f (m2). This is sometimes called weak collision resistance.

A function f is (strong) collision resistant if it is hard to find two messages m1 and m2 such that f (m1) = f (m2).

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

A function f is preimage resistant if, given h, it is hard to find any m such that h = f (m).
A function f is second preimage resistant if, given an input m1, it is hard to find m2 6= m1 such that f (m1) = f (m2).

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 confiden tiality?

Because of the following reason:
-In a document retrieval system containing legal records, it may be important to know that the copy retrieved is identical to that stored.
-In a secure communications system, the correct transmission of messages may override confidentiality concerns.

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

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

A cryptographic hash function “binds” the bytes of a file together in a way that makes any alterations to the file apparent.

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

# Lecture 51

1. For key exchange, if S wants to send key K to R, can S send the following message: $\{\{K\}_{KS^{-1}}\}_{KR^{-1}}$ ? Why or why not?
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?

It's fine because S could have performed the inner encryption, so authentication is accomplished.

3. Is $\{\{\{K\}_{KS^{-1}}\}_{KR}\}_{KS}$ equivalent to $\{\{K\}_{KS^{-1}}\}_{KR}$ ?

Yes

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

Key exchange requires both confidentiality and authentication.

# Lecture 52

1. What would happen if g, p and $G^A \bmod P$ were known by an eavesdropper listening in on a Diffie-Hellman exchange?

Alice chooses a secret number a, and sends Bob.

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?