Aaron Dishman
UTID: adishman
UTCS: adishman
email: aaron.dishman@utexas.edu

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?

    Because if you get greater than C/h, you have a number greater than the defined entropy. If that is the case, you have miscalculated your entropy.

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

    Because noise can result in a message not being received, but increasing the redundancy(like repetitiveness) will mean that a message will eventually get 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?

    h = -(log 1/10)

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

    because different letters happen at different frequencies

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

    zero order doesn't take into account how often the letters actually occur in a language

    first order does

    second order takes into account how often pairs of letters happen

    third-order takes into account how often triplets of letters occur

Lecture 36

1. Why are prior probabilities sometimes impossible to compute?

    because knowing what happened before you entered the conversation is not always possible.

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

Because a given message most likely contains information related to information that both parties already know or have discussed. If an observer is not aware of such prior information, the current messages information might hold no meaning.

3. Explain the relationship between entropy and redundancy.

entropy can be a measure of the amount of redundancy.

Lecture 37

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

there are no letters, just numbers and symbols - might indicate simple substitution

the number 8 looks like it appears the most - could be related to most common letter of the encrypted messages original language

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

so that there is a way to decipher the encrypted message…the point of encryption being to hide information, not destroy it

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

hides it from people that don't have the key

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

repetitive characters that stay in an encrypted text can directly correlate to repetitive characters in the encrypted texts' original language

Lecture 38

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

P

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

C = {P}KE

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

they might notice that when a crisis is happening, there seems to be more of a certain pattern of messages occurring, indicating a possible cause…

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

frequency of letters in a given language could be an indicator of how to break an encryption algorithm.

Lecture 39

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

   because it may take so much time that an analyst won't live long enough to realize the break

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 2^{n-1} operations?

   because if you do a linear search on the entire keyspace, on average you will find the correct key halfway through your linear search

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

   in combination, it makes breaking of encryption relatively difficult

4. Explain the difference between confusion and diffusion.

   confusion is like substituting one letter for another uniformly across a given text.
   diffusion is like moving a given letter to a different position in a given text.

5. Is confusion or diffusion better for encryption?

   neither is better, both working in conjunction is best for encryption

Lecture 40

1. What is the difference between mono-alphabetic and poly-alphabetic substitution?

   mono-alphabetical : substitution is done uniformly
   poly-alphabetical : different substitutions depending on where in plaintext the symbol occurs

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

   could be a table; depends on you.

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

   because of the nature of possibilities in a given alphabets' number of letters

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?

   the number of letters in the alphabet -= 1

6. Is the Caesar Cipher algorithm strong?

not especially

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

Lecture 41

1. Why are there 17576 possible decryptions for the “xyy” encoding on slide 3?
because the alphabet contains 26 letters, and there is a 3 letter encoding, so maths => 26^3 = 17576

2. Why is the search space for question 2 on slide 3 reduced by a factor of 27?
because if it’s simple substitution, that means that the letter wouldn’t be substituted with itself.

3. Do you think a perfect cipher is possible? Why or why not?
it is possible, think one-time pad, but is not always usable

Lecture 42

1. Explain why the one-time pad offers perfect encryption.
The key is that same length as the plaintext, so by XORing it, not information can be gleaned from the encrypted text

2. Why is it important that the key in a one-time pad be random?
If not, it could provide clues as to how the key gets chosen

3. Explain the key distribution problem.
for symmetric keys, each pair needs a private key. so for n users, you need n! - 1 keys.

Lecture 43

1. What is a downside to using encryption by transposition?
Not strong by themselves

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: how to get keys to everyone that needs to securely communicate with one another
key management: how to preserve there safety and make them available

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

No, because you need the private key to decrypt

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

they each have their advantages and disadvantages in different contexts

Lecture 45

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

block ciphers result in stronger encryptions

2. What is the significance of malleability?

If you can change something in an encrypted text, the same change can be seen in the plaintext…allows for possible code breaking

3. What is the significance of homomorphic encryption?

a form of encryption which allows specific types of computations on a cipher text to show up in plaintext, therefore, relates to malleability

Lecture 46

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

subBytes: for every byte, substitute it with a value stored in the location of a 256 element lookup table

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?

shiftRows: 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.

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

Inverting the MixColumns step requires multiplying each column by the inverse of the array used to encrypt.

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

The block positions are used for substitution of values in a 256 element lookup table

The rounds are used to make breaking of the encryption sufficiently difficult

5. Why would one want to increase the total number of Rounds in AES?
To increase confusion and diffusion even more.

Lecture 47

1. What is a disadvantage in using ECB mode?
patterns can still be seen after encryption

2. How can this flaw be fixed?
Perform some sort of function to “randomize” blocks before they are encrypted

3. What are potential weaknesses of CBC?
Observed changes: An attacker able to observe changes to cipher text over time will be able to spot the first block that changed.
Content Leak: If an attacker can find two identical cipher text blocks, Ci and Cj, he can derive the following relation: $Ci-1 \oplus Cj-1 = Pi \oplus Pj$, and derive information about two plaintext blocks.

4. How is key stream generation different from standard block encryption modes?
It is really fast, because you are doing simple substitution one character at a time but this also means that it is easier to break

Lecture 48

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

2. Why are one-way functions critical to public key systems?
because it’s easily computable as well as difficult to invert without additional information.

3. How do public key systems largely solve the key distribution problem?
by reducing the number of keys required to ensure authentication and confidentiality

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 more computationally 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?

yes, because either key can be used to encrypt for the other one to decrypt

2. Explain the role of prime numbers in RSA.

two prime numbers are required for generating a RSA key pair. If you are able to factorize the public key and find these prime numbers, you will then be able to find the private key.

3. Is RSA breakable?

Yes

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

because only a has her private key to decrypt

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

because b didn't encrypt with his private key

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

because a can decrypt with B's public key

7. How can someone intercepting $\{M\}_{K-1b}$ read the message?

by decrypting with his public key

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

{{M}K-1A}KB

Lecture 50

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

For ease of accessibility.

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

Strong collision resistance means it is hard to find two messages that a hash function will map to the same value

Weak collision resistance is when a function f is second preimage resistant, therefore if, given an input m1, it is hard to find m2 = m1 such that f(m1) = f(m2).

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

preimage resistant: hard to find a message that hashes to a given hash value.

second preimage resistant: its hard to find message different from a given message that hashes to the same hash value

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

You have to iterate through 1.25 * 2^64 hash values before finding a collision

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

You have to iterate through 1.25 *2^80 hash values before finding a collision

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

Hash functions can't be used to encrypt and decrypt data because it isn't possible to recreate the original message from a hash value. Since you are going from an infinite source of messages to a finite number of hash values it is impossible to accurately recreate the original message.

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

The attribute of preimage resistance.

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

Hash a message then use RSA public key to encrypt it before transmitting. On the other side the recipient could decrypt it with the private key then apply the hash function on the message to make sure the file had not changed.

Lecture 51

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

No, because S would not have access to R's private key.

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 anyone could strip the outer level of encryption, and R would not know that S was the sender.

3. Is $\{\{\{\mathbf{K}\}_{K_{S^{-1}}}\}_{K_R}\}_{K_S}$ equivalent to $\{\{\mathbf{K}\}_{K_{S^{-1}}}\}_{K_R}$?

No

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

Confidentiality and authentication, because the keys need to be secure and you need to know who the sender is.

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?

Nothing, they can't determine the key from this information.

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

If the value of 'a' was discovered, the eavesdropper they would be able to determine the key

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

They would be able to determine the key by intercepting Alice's transmission of (g^a mod p)