Name: Luis C. Lopez
EID: LL9338
CS Login: LL9338
Email: lclg21@utexas.edu

CS361 Questions: Week 3

Lecture 34

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

To do so would imply that you had an encoding which compressed beyond entropy in the language.

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

Because the message would better be able to be transmitted due to its repeated characters.

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?

$h = -(\log 1/10) = 3.32$

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

Because natural languages contain significant redundancy and it would require a more complex model and still just be able to get an estimate of the entropy.

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

Zero-order model: Each character is independent of all other characters all possible values in the alphabet are equally likely to occur.

First-order model: The characters are still independent of one another, but the probability distribution of the characters are according to their frequencies.

Second-order model: the probability distribution of the character varies according to according to what the previous character was.

Third-order model: Same as second-order model but the present character depends on the previous two characters.

Lecture 36

1. Why are prior probabilities sometimes impossible to compute?

Because the information content of the message changes and it depends on the state of knowledge of the receiver.

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

The more the listeners knows, the less information you need to convey to reduce the uncertainty.

Name: Luis C. Lopez
EID: LL9338
CS Login: LL9338
Email: lclg21@utexas.edu

3. Explain the relationship between entropy and redundancy.

Entropy can be used to measure the amount of redundancy in the encoding. The less the redundancy in the plaintext, the harder to code.

Lecture 37

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

Try to analyze the type of language is trying to encode. How many characters it has and which ones are shown more frequent.

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

Because we might consider the shift amount to be fixed for a given version, and that would be consider a keyless cipher.

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

The effect of encrypting a file is to hide the information content but not to destroy it.

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

If redundancy is preserved in the source text, the attacker can use those to get some leverage on decrypting the text.

Lecture 38

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

D (E (P)))

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

D (E (P, KE), KD)

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

It can give some clues about the message without the cryptanalyst even knowing what the message is about.

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

Because of the redundancy of the language. It can have patterns in which potentially a cryptanalyst can decode.

Name: Luis C. Lopez
EID: LL9338
CS Login: LL9338
Email: lclg21@utexas.edu

Lecture 39

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

Because even though an encryption algorithm can be decoded, the analyst can try all keys systematically but it will take so long to find the right answer so the analyst must be able to recognize the right answer to the algorithm.

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 we would try all the keys on by one until finally recovering K but it would take a lot of operations to get K.

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

In combination, transposition and substitution are very powerful because substitution tends to be good at confusion and transposition tends to be good at diffusion.

4. Explain the difference between confusion and diffusion.

Confusion transforms information in plaintext so that an interceptor cannot readily extract it. Diffusion spreads the information from a region of plaintext widely over the ciphertext.

5. Is confusion or diffusion better for encryption?

Yes, because it makes it harder for an individual to extract the content that easily.

Lecture 40

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

Monoalphabetic substitution is when each symbol of the plaintext is exchanged for another symbol uniformly. Polyalphabetic substitution is when the substitutions are made depending on where in the plaintext the symbol occurs.

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

It depends how we specify the mapping. i.e. a table.

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

Because there are only a finite number of such tables, so k! will depend on the size of the alphabet.

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

26

6. Is the Caesar Cipher algorithm strong?

No

Name: Luis C. Lopez
EID: LL9338
CS Login: LL9338
Email: lclg21@utexas.edu

7. What is the corresponding decryption algorithm to the Vigenere ciphertext example?
Decryption is performed by going to the row in the table corresponding to the key, finding the position of the cipher text in this row, and then using the column's label as the plaintext.

Lecture 41

1. Why are there 17576 possible decryptions for the "xyy" encoding on slide 3?
Because xyy is a substitution cipher and there are 26 letters in the alphabet and 3 symbols to decipher. So 26^3 = 17576.

2. Why is the search space for question 2 on slide 3 reduced by a factor of 27?
Because since now it is a simple substitution cipher, there are 26 x 25 = 650 decryptions possible, so we decrease from 17,576 to 650, which is a reduce search space by a factor of 27.

3. Do you think a perfect cipher is possible? Why or why not?
Yes, because a perfect cipher would require as many possible keys as plaintexts, with the key chosen randomly.

Lecture 42

1. Explain why the one-time pad offers perfect encryption.
Because if an attacker intercepts the ciphertext and knows that a one-time pad is in use, 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?
Because if we knew something about the key, then the cipher would no longer be a perfect cipher.

3. Explain the key distribution problem.
Is about how to communicate securely between the sender and the receiver. How can the sender and the receiver agree on a secret key if they need to communicate without letting the attackers know of a way to get the key.

Lecture 43

1. What is a downside to using encryption by transposition?
That transposition preserves letter frequencies but not diagrams or trigrams, etc.

Name: Luis C. Lopez
EID: LL9338
CS Login: LL9338
Email: lclg21@utexas.edu

Lecture 44

1. Is a one-time pad a symmetric or asymmetric algorithm?
Is a symmetric algorithm because it uses the same key for both encryption and decryption.

2. Describe the difference between key distribution and key management.
Key distribution is how we convey keys to those who need them to establish secure communication. Key management is when given a large number of keys, is how 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?
No, because Ks is a public key and in order to decrypt S's message we need the private key.

4. Are symmetric encryption systems or public key systems better?
Public key systems are better because each individual requires two keys, so for n individuals, 2n keys are required and for a symmetric encryption, n(n - 1) / 2 keys are required.

Lecture 45

1. Why do you suppose most modern symmetric encryption algorithms are block ciphers?
Because they encrypt a group of plaintext symbols as one block, like 64 bits for DES, 128 bits for AES, etc.

2. What is the significance of malleability?
With malleability we are able to manipulate ciphertext with predictable effects on plaintext.

3. What is the significance of homomorphic encryption?
It can be used to create secure voting systems, collision-resistant hash functions, and private information retrieval schemes. Homomorphic encryption schemes are malleable by design.

Lecture 46

1. Which of the 4 steps in AES uses confusion and how is it done?
subBytes uses confusion by replacing the byte by the value stored in the table.

2. Which of the 4 steps in AES uses diffusion and how is it done?
shitRows uses diffusion because it shifts the rows to the left certain amount of bytes according to the row.

3. Why does decryption in AES take longer than encryption?
Because the mixColumns step requires multiplying each column by a fixed array.

Name: Luis C. Lopez
EID: LL9338
CS Login: LL9338
Email: lclg21@utexas.edu

4. Describe the use of blocks and rounds in AES.
   With AES, the input is fixed in size blocks and the operations are performed repeatedly like a state. So the key is arranged as a 4 x n array of bytes and is initially expanded in a recursive process into r + 1 128-bit keys, and where r is the number of rounds.

5. Why would one want to increase the total number of Rounds in AES?
   Because the more rounds there are would mean more security against cryptanalysts because there would be more confusion and diffusion.

Lecture 47

1. What is a disadvantage in using ECB mode?
   Each block in the plaintext, the result will be identical block as the ciphertext.

2. How can this flaw be fixed?
   We would fix it by randomizing the blocks before they are encrypted.

3. What are potential weaknesses of CBC?
   Some potential weaknesses are that an attacker might be able to observe changes to ciphertext and If the attacker can find two identical ciphertext blocks, he can derive information about the two plaintext blocks.

5. How is key stream generation different from standard block encryption modes?
   In Key stream generation the result is a key stream that can be used as in one-time pad.

Lecture 48

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

2. Why are one-way functions critical to public key systems?
   Because a one-way functions are easy to compute but hard to invert.

3. How do public key systems largely solve the key distribution problem?
   Because we can give out the public key and anybody can use it to encrypt but they would not be able to decrypt it because they would need the private key, which only the sender has.

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

5. Compare the efficiency of asymmetric algorithms and symmetric algorithms.
   Asymmetric algorithms require 2n keys. Symmetric algorithms n(n - 1) / 2 keys.

Name: Luis C. Lopez
EID: LL9338
CS Login: LL9338
Email: lclg21@utexas.edu

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 work, but any one would be able to read the message.

2. Explain the role of prime numbers in RSA.
The prime numbers works knapsack problem, where a set of integers and a target sum is given to find a subset of the integers that sum to the target, which is theoretically very secure.

3. Is RSA breakable?
Yes, RSA is breakable.

4. Why can no one intercepting {M}Ka read the message?
Because only A has the key which will allow the decryption of the message.

5. Why can't A be sure {M}Ka came from B?
Because any one might have A's public key.

6. Why is A sure {M}K−1b originated with B?
Because no one has the private key but B.

7. How can someone intercepting {M}K−1b read the message?
By just knowing the public key.

8. How can B ensure authentication as well as confidentiality when sending a message to A?
By having two pair of keys, one pair for privacy and the other for authenticity.

Lecture 50

1. Why is it necessary for a hash function to be easy to compute for any given data?
Because it converts variable-size text into a small datum, usually a fixed size integer.

2. What is the key difference between strong and weak collision resistance of a hash function.
Ina string collision, it is hard to find two messages m1 and m2 such that f(m1) = f(m2). And weak collision, 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?
In preimage resistant, given hash function, it is hard to find any m such that h = f(m). And second preimage resistance is the same thing as weak collision.

4. What are the implications of the birthday attack on a 128 bit hash value?
It would take longer to find a collision.

Name: Luis C. Lopez
EID: LL9338
CS Login: LL9338
Email: lclg21@utexas.edu

5. What are the implications of the birthday attack on a 160 bit hash value?
It would take even longer than a 128 bit hash value to find a collision.

6. Why aren't cryptographic hash functions used for confidentiality?
Because hash functions are used more for integrity purposes. The transmission of messages may override confidentiality concerns and we don't want that.

7. What attribute of cryptographic hash functions ensures that message M is bound to H(M), and therefore tamper-resistant?
By sealing the file we make it tamper-proof. So 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?
By keeping a private key and using cryptographic hash functions to ensure confidentiality and integrity respectively.

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−1R Why or why not?
No because S is sending it with two private keys making R able to decode the message.

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 by doing the encryption in the other order it would not have confidentiality and/ or integrity.

3. Is {{{K}KS−1}KR}KS equivalent to {{K}K−1S}KR?
Yes, if it was KR-1 then R would be able to decrypt the message.

4. What are the requirements of key exchange and why?
Key exchange requires both confidentiality and authentication so that the cipher wont be able to be detected or changed.

Lecture 52

1. What would happen if g, p and ga mod p were known by an eavesdropper listening in on a Diffie-Hellman exchange?
It would take longer than lifetime to crack the message.

Name: Luis C. Lopez
EID: LL9338
CS Login: LL9338
Email: lclg21@utexas.edu

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

    Nothing because the earsdropper would still need the prime number p and the base g to come up with something helpful.

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

    Nothing because the earsdropper would still need the prime number p and the base g to come up with something helpful.