Questions Week 3

Matt Hendrickson
mjh2793
mjh2793
matthewjames@utexas.edu

Lecture 34

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

You will always have that C/h - epsilon. the epsilon can be arbitrarily small

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

an increased redundancy means you have a lower entropy. Having a lower entropy means you can always stay under the capacity, C given by Shannon's Theorem of Noisy Channels.

Lecture 35

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

10*((1/10)*(logbase2(1/10))

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

Multiple words have the same meaning.

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

the zero order model assumes every symbol is equally likely.
First order model assumes each symbol is independent of one another.
Second order model calculates english based on groupings of letter by two.
third order does the same but by groups of three

Lecture 36

1. Why are prior probabilities sometimes impossible to compute?

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

the content of the message can be interpreted differently by the observer depending on his knowledge of the message.

3. Explain the relationship between entropy and redundancy

entropy can be used to measure the amount of redundancy in a message.

Lecture 37

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

Captain Kidd’s encrypted message.
It was written by a pirate so probably a simple encryption.
It will have directions because message is most likely to a treasure

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

3. What effect does encrypting a file have on its information content?
It hides a message, duh
4. How can redundancy in the source give clues to the decoding process?
It shows what characters/phrases are more commonly used.

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, KE), KE), KD).
D(E(C, KE), KD)
3. Why might a cryptanalyst want to recognize patterns in encrypted messages?
It can show where the redundancies are
4. How might properties of language be of use to a cryptanalyst?
Things like spaces can show where each word is. Certain words might show where things of importance are.

Lecture 39

1. Explain why an encryption algorithm, while breakable, may not be feasible to break?
It may take too long.
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 2n−1 operations?
many ciphers use an n-bit string as their key. That is how many operations is required to find every possible key.
3. Explain why substitution and transposition are both important in ciphers.
They provide the properties of confusion and diffusion. they change the message to something not readily interpretable and then spread that message around, respectively.
4. Explain the difference between confusion and diffusion.
^^
5. Is confusion or diffusion better for encryption?
both are necessary. almost all modern commercial symmetric ciphers use some combo of the two

Lecture 40

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

mono - where each symbol is exchanged for another based on a single key.
poly - where each symbol is exchanged for another but use few or many different keys depending on where the symbol occurs on the plaintext.

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

The algorithm that maps one letter onto another.

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

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

a number for the distance away each cyphertext symbol is from its plaintext symbol.

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

one/two numbers assuming a character set that has more than ten letters (double digits)

6. Is the Caesar Cipher algorithm strong?

no

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

because the encryption goes on a plain + key = cypher, use the same properties of “addition” used in the encryption process and do cypher - key = plain.

Lecture 41

1. Why are there 17576 possible decryptions for the “xyy” encoding on slide3?

3 letters each with 26 possiblitites

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

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

No, If they know the encryption algorithm then they can see at least a small portion of how the plaintext is encrypted and work backward from there. unless the encryption algo is also encrypted lol.

Lecture 42

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

Even if you know the cyphertext and that the one time pad is being used, you cannot eliminate any possible key as the correct one. The XOR operation guarantees that.

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

3. Explain the key distribution problem.

If they already have a secure channel to distribute the key then why still have a cypher?
If they don’t, then how can distribute the key securely?

Lecture 43

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

Since the transposition requires a number to shift everything simply iterate through some set of numbers you think they key number falls in the range of while trying to decrypt with each number.

Lecture 44

1. Is a one-time pad a symmetric or asymmetric algorithm?
its symmetric. one time pad uses the same kley for encryption and decryption
2. Describe the difference between key distribution and key management.
key distribution - the problem of giving the keys to those who need them
key management - given a large number of keys, how do we preserve their safety and make them available when needed.
3. If someone gets a hold of Ks, can he or she decrypt S's encrypted messages? Why or why not?
If that means that someone got EVERY key then yes, but they would just have to try them until they found the one they were looking for.
4. Are symmetric encryption systems or public key systems better?
they are mostly incomparable. Going back to the first week, it would depend on the context.

Lecture 45

1. Why do you suppose most modern symmetric encryption algorithms are block ciphers?
It is easy to detect an intruder inserting symbols
2. What is the significance of malleability?
Someone could mess with the cyphertext to corrupt the data held within the plaintext
3. What is the significance of homomorphic encryption?

Lecture 46

1. Which of the 4 steps in AES uses confusion and how is it done?
SubBytes - use the bytes value as an index into a lookup table, then replace with that value
mixColumns - for each column of the state multiply by a fixed 4x4 matrix of integers
2. Which of the 4 steps in AES uses diffusion and how is it done?
shiftRows - Let Ri denote the ith 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.
3. Why does decryption in AES take longer than encryption?
the decryption version of Mixcolumns means using a matrix multiplication, something that is expensive to implement.
4. Describe the use of blocks and rounds in AES.
The program reads in a 128 bit and arranges them as a 4 x 4 array of bytes.
5. Why would one want to increase the total number of Rounds in AES?
make it more encrypted?

Lecture 47

1. What is a disadvantage in using ECB mode?

It is simple. You use the same key on each “block” of data

2. How can this flaw be fixed?

randomize the blocks before you encrypt them

3. What are potential weaknesses of CBC?

It can be watched over time to figure out the plaintext

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

Lecture 48

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

The decryption key

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

So you can’t just invert the public encryption to decrypt.

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

Everyone gets one 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.

Asymmetric encryptions take longer to perform because they rely less on simple bit-wise operations. Symmetric ops use a lot of bitwise manipulations so they are a lot more efficient timewise

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, that is form lecture 48.

2. Explain the role of prime numbers in RSA.

3. Is RSA breakable?

Yes

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

They don’t have the decryption algorithm, K-1a. Only A has the decryption.

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

Because everyone has access to A’s encryption key, Ka.

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

Because B is the only person that has access to K-1b.

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

They would just need the Kb key whih is available publicly.

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

message to A?

B knows that only A can read the message because A is the only person that has the key.
If B encrypts

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.

weak - if you have a message m1 its hard to find another message m2 s.t. f(m1) = f(m2)
strong - its hard to find ANY two messages s.t. f(m1) = f(m2)

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

preimage resistance means its difficult to find a message, m, s.t h = f(m) when you are given the hash value, h. Basically it means that the hash function, f is hard to invert.

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?

They are designed not to be decrypted. One person hashes a file and stores the result. Later they can hash the file again and compare with the stored result and see if it has been changed.

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

seal

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

Both A and B need a hash function f, that only they have. B hashes a message and sends the value, v and the message, m1 after encrypting it with A's public encryption algo. A decrypts the message and value and then hashes the message and compares with the value. The only vulnerability is making sure that ONLY A and B have the hash function.

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,

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?

Yes,

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

4. What are the requirements of key exchange and why?
You have to agree on a key exchange.

Lecture 52

1. What would happen if g, p and g^a mod p were known by an eavesdropper listening in on a Diffie-Hellman exchange?
The eavesdropper would not be able to find out the secret code.
2. What would happen if a were discovered by an eavesdropper listening in on a Diffie-Hellman exchange?
Then they could find out the shared number
3. What would happen if b were discovered by an eavesdropper listening in on a Diffie-Hellman exchange?
^^