Brian Chow
EID/CS login: bc23784
Email: brianj.chow@yahoo.com
CS 361 (90155)
For 06/26/14

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?
   1. That would mean doing better than the entropy of the language, which contradicts the entire premise of entropy.
2) How can increasing the redundancy of the coding scheme increase the reliability of transmitting a message over a noisy channel?
   1. It can reduce the number of errors encountered due to the noise over the channel.

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?
   1. h = -(log 1/10)
2) What are reasons why computing the entropy of a natural language is difficult?
   1. Characters/symbols don't occur in equal proportions, and entropies can differ when using 2nd, 3rd, nth-order models.
3) Explain the difference between zero, first, second, and third-order models.
   1. The zero-order model assumes all symbols have an equal probability of occurring. The first-order model is a step above the zero-order model, and accounts for different probabilities for different symbols. The second-order model introduces the concept of a symbol commonly occurring after another symbol, and the third-order model builds upon this by adding another symbol into the mix.

Lecture 36

1) Why are prior probabilities sometimes impossible to compute?
   1. Entropy can be relative to a particular person or thing; often there is no accurate way of (knowing how to) compute prior probabilities.
2) Why is the information content of a message relative to the state of knowledge of an observer?
   1. Not everyone has the exact same brain with the exact same knowledge of the exact same subjects. A message in Russian is useless to anyone who doesn't know the Cyrillic alphabet.
3) Explain the relationship between entropy and redundancy.
   1. Entropy “can be used to measure the amount of 'redundancy' in the encoding.” There is no redundancy if “the information content of a message is equal to the length of the encoded message.”

Lecture 37

1) List your observations along with their relevance to cryptography about Captain Kidd's encrypted message.
    1. The language is most likely English, which allows us to make better guesses as to the entropy of the language (frequencies/probabilities of characters, etc). Most likely the encryption would be simple, along the lines of simple substitution.
2) Explain why a key may be optional for the processes of encryption or decryption.
    1. Depending on the encryption algorithm used, a key may not be necessary to decrypt the message (a weak example would be Huffman encoding).
3) What effect does encrypting a file have on its information content?
    1. It creates a "systematically noisy channel", making it more difficult to properly read a plaintext message.
4) How can redundancy in the source give clues to the decoding process?
    1. Redundancy "provides leverage to the attacker", and can be used to observe differences in the information content in order to make a more accurate guess of the decrypted message.

Lecture 38

1) Rewrite the following in its simplest form: D(E(D(E(P)))).
    1. C = E(D(E(P))), P = D(C)
2) Rewrite the following in its simplest form: D(E(E(P, K_E), K_E), K_D).
    1. E(P, K_E)
3) Why might a cryptanalyst want to recognise patterns in encrypted messages?
    1. S/he can use it to see if there's any rhyme or reason as to what triggers (some part of) the pattern, which could lead to the discovery of a vulnerability that needs to be patched.
4) How might properties of language be of use to a cryptanalyst?
    1. They can be used to help reduce redundancy, making it somewhat simpler to decode a message (using relative probabilities of characters/symbols/etc).

Lecture 39

1) Explain why an encryption algorithm, while breakable, may not be feasible to break?
    1. It may take an extremely long amount of time (several lifetimes) to find the correct key, especially when "trying all keys systematically."
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?
    1. Given an *n*-bit string, there are 2^{n-1} invalid keys (^2 possibilities per bit in the string).
3) Explain why substitution and transposition are both important in ciphers.
    1. Together they can provide the valuable properties of confusion and diffusion.
4) Explain the difference between confusion and diffusion.
    1. Diffusion is distributing the encrypted information across a large amount of the ciphertext; confusion is encrypting the information so that "an interceptor cannot readily extract it."
5) Is confusion or diffusion better for encryption?
    1. Diffusion - if the ciphertext is sufficiently large, there may be too many places to search for pieces of information for a brute-force attack to be feasible. Confusion isn't very helpful if

the encryption methods are poor.

Lecture 40

1) What is the difference between monoalphabetic and polyalphabetic substitution?
    1. The former applies to when plaintext symbols are uniformly exchanged with another; the latter applies to when “different substitutions are made depending on where in the plaintext the symbol occurs.”
2) What is the key in a simple substitution cipher?
    1. The reverse mapping.
3) Why are there k! mappings from plaintext to ciphertext alphabets in simple substitution?
    1. For every letter, there are *k* - (# assigned possibilities) possibilities; compute the factorial to determine the total number of possibilities.
4) What is the key in the Caesar Cipher example?
    1. The distance to the “right” or “left” to which each plaintext character is mapped.
5) What is the size of the keyspace in the Caesar Cipher example?
    1. 26!
6) Is the Caesar Cipher Algorithm strong?
    1. No. There are only a comparatively small number of possibilities that a brute-force attacker would have to check (26!).
7) What is the corresponding decryption algorithm to the Vigenere ciphertext example?
    1. Map each combination of two letters in the alphabet to one other letter.

Lecture 41

1) Why are there 17576 possible decryptions for the “xyy” encoding on slide 3?
    1. There are 26 possible letters that each character in the string can represent. The probability of guessing the correct decryption is 1 / (26 ^ 3).
2) Why is the search space for question 2 on slide 3 reduced by a factor of 27?
    1. It is a simple substitution, so there are only (26 * 25) total encryption possibilities (vs 26 * 26).
3) Do you think a perfect cipher is possible? Why or why not?
    1. Not practically. It would seem the best bet is to create a cipher that would take centuries to crack.

Lecture 42

1) Explain why the one-time pad offers perfect encryption.
    1. There is no possible reduction in the number of plausible keys there are (so they must all be tried).
2) Why is it important that the key in a one-time pad be random?
    1. There will be no patterns or redundancy that an attacker could use to potentially decrypt it.
3) Explain the key distribution problem.
    1. If the channel used by a sender and a receiver is already secure, there is no need for a key, but if it is not secure, there is no means of transmitting the key securely in order to establish the secured channel.

Lecture 43

1) What is a downside to using encryption by transposition?
    1. Frequencies of individual letters are still preserved; they are just in a different order.

Lecture 44

1) Is a one-time pad a symmetric or asymmetric algorithm?
    1. Symmetric algorithm.
2) Describe the difference between key distribution and key management.
    1. The former relates to confidentiality, and the latter relates to integrity and availability.
3) If someone gets a hold of Ks, can he or she decrypt S's encrypted messages? Why or why not?
    1. No. Ks's key is publicly available for message transmission; it does not allow for decryption of a message.
4) Are asymmetric encryption systems or public key systems better?
    1. Neither; they each have their own benefits and applications. For instance, public key would work great with a large number of independent users, whereas a secret key must be shared between each pair of users in symmetric encryption.

Lecture 45

1) Why do you suppose most modern symmetric encryption algorithms are block ciphers?
    1. They offer a much higher level of security than stream ciphers, which suffer from low diffusion (all information is in one place) and high susceptibility to modification.
2) What is the significance of malleability?
    1. Achieving non-malleability means that the ciphertext can't be manipulated to produce a change in the plaintext (“reverse-engineering” it).
3) What is the significance of homomorphic encryption?
    1. It allows the development of collision-resistant hash functions.

Lecture 46

1) Which of the 4 steps in AES uses confusion and how is it done?
    1. Step 3; the state is multiplied with a fixed 4x4 matrix.
2) Which of the 4 steps in AES uses diffusion and how is it done?
    1. Step 2; row transposition.
3) Why does decryption in AES take longer than encryption?
    1. Inverting the third (MixColumns) step requires costly ~O(n^2) matrix multiplication.
4) Describe the use of blocks and rounds in AES.
    1. The blocks contain the input (plaintext), and the algorithm is implemented in rounds (“perform similar operations repeatedly to a 'state'”).
5) Why would one want to increase the total number of rounds in AES?
    1. As the number of rounds increases, so does the number of operations performed on a state, potentially allowing for better encryption.

Lecture 47

1) What is a disadvantage in using ECB mode?
   1. Blocks that are identical in the plaintext will also be identical in the ciphertext.
2) How can this flaw be fixed?
   1. Attempt to randomize the blocks before they are encrypted (e.g., XOR a block with a block surrounding it).
3) What are potential weaknesses of CBC?
   1. Two identical ciphertext blocks can be analyzed to determine why two different blocks formed the same ciphertext block, and watching the ciphertext to see which block changes over time can help an attacker establish a pattern during/for the encryption.
4) How is key stream generation different from standard block encryption modes?
   1. The output appears to be random in both, but the plaintext can be recovered using key stream generation, as opposed to standard block encryption modes.

Lecture 48

1) For public key systems, what must be kept secret in order to ensure secrecy?
   1. The decryption key.
2) Why are one-way functions critical to public key systems?
   1. They are easy to compute (for encryption), but very difficult to invert (for decryption) with no further information.
3) How do public key systems largely solve the key distribution problem?
   1. Use the public key to encrypt in the secure domain and the secret key to decrypt in the unsecure domain.
4) Simplify the following according to RSA rules: $\{\{\{P\}_{K}^{-1}\}_{K}\}_{K}^{-1}$.
   1. $\{P\}_{k}^{-1}$
5) Compare the efficiency of asymmetric algorithms and symmetric algorithms.
   1. Asymmetric algorithms and one-way functions guarantee that a “simple” brute-force attack will still take an unfeasibly long amount of time due to the difficulty of inverting a one-way function (vs ordinary bitwise operations).

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?
   1. Yes, since the algorithm is symmetric in its use of keys.
2) Explain the role of prime numbers in RSA.
   1. It would take a long time for an attacker to factor a very large prime number to obtain the decryption key, whereas the legitimate receiver would merely have to do a much simpler computation to decrypt.
3) Is RSA breakable?
   1. Yes, but usually not in a feasible timespan.
4) Why can no one intercepting $\{M\}_{Ka}$ read the message?
   1. Because A is the only person who has the proper private key to decrypt the message.
5) Why can't A be sure $\{M\}_{Ka}$ came from B?

    1. The public key is, as its name suggests, public, and can come from anyone other than B.

6) Why is A sure $\{M\}K_b^{-1}$ originated with B?
    1. B is the only person who could transmit a message with the particular private key being used.
7) How can someone intercepting $\{M\}K_b^{-1}$ read the message?
    1. Use the public key that B used.
8) How can B ensure authentication as well as confidentiality when sending a message to A?
    1. Use two keys - one for the message itself, and one as a digital signature that can verify that the message came from him (B).

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?
    1. Weak - m_2 cannot equal m_1. Strong - m_2 can equal m_1.
3) What is the difference between preimage resistance and second preimage resistance?
    1. In preimage resistance, one only has to solve for the missing variable (the expected output of the function is given). In second preimage resistance, the expected output is not given, and two different values for the function variable must have the same function output.
4) What are the implications of the birthday attack on a 128-bit hash value?
    1. On average, it takes 1.25(sqrt(128)) tries to find a collision.
5) What are the implications of the birthday attack on a 160-bit hash value?
    1. On average, it takes 1.25(sqrt(160)) tries to find a collision.
6) Why aren't cryptographic hash functions used for confidentiality?
    1. They are far more useful in maintaining integrity by, for example, alerting users to the modification of a file. They don't necessarily handle read permission access to objects.
7) What attribute of cryptographic hash functions ensures that message M is bound to *H*(*M*), and therefore tamper-resistant?
    1. They “'bind' the bytes of a file together in a way that makes any alterations apparent.” Any change or difference would be reflected in a different hash for the same file.
8) Using RSA and a cryptographic hash function, how can B securely send a message to A and guarantee both confidentiality and integrity?
    1. B can send a message to A using RSA (K_a) along with a hash of the message. A can compute the hash for the received message and compare it with the hash B provided in order to check for tampering.

Lecture 51

1) For key exchange, if S wants to send K to R, can S send the following message: $\{\{K\}\{_{KS-1}\}_{KR-1}$? Why or why not?
    1. No; both levels of encryption can be decrypted through the use of public keys.
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?
    1. Not without risking the message being compromised (R is not the only person capable of decrypting it).
3) Is $\{\{\{K\}_{KS-1}\}_{KR}\}_{KS}$ equivalent to $\{\{K\}_{KS-1}\}_{KR}$?

    1. No; the former requires R and S to both decrypt, while the latter only requires R.
4) What are the requirements of key exchange and why?
    1. Confidentiality and authentication, to ensure that the sender and receiver did in fact intend to transmit information to each other and that the traffic hasn't been intercepted.

Lecture 52

1) What would happen if *g*, *p*, and g^amod*p* were known by an eavesdropper listening in on a Diffie-Hellman exchange?
    1. S/he wouldn't be able to determine the value in the message.
2) What would happen if *a* were discovered by an eavesdropper listening in on a Diffie-Hellman exchange?
    1. S/he would be able to determine the value in the message.
3) What would happen if *b* were discovered by an eavesdropper listening in on a Diffie-Hellman exchange?
    1. S/he would be able to determine the value in the message.