Name: michael truong
EID: mkt532
CS Login: mtruong
Email: mtruong92@utexas.edu

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 entrophy h (bits per symbol) and a channel can trasmit c bits per second, then 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, your friend on the other side of the room, you may have to shout at him a thousand times, but eventually you'll get the message through

Lecture 35

1. If we want to transmit a sequence of the digits 0-9. According to the zeroorder model, what is the entropy of the language?
3.32193

2. What are reasons why computing the entropy of a natural language is difficult?
characters are not equally likely, symbols are not independent of one another

3. Explain the difference between zero, first, second and third-order models.
zero: assume that all characters are equally likely;
first: assume that all symbols are independent of one another, but are not equally likely;
second: doesn't assume that all digrams are equally likely;
third: doesn't assume that all trigrams are equally likely;

Lecture 36

1. Why are prior probabilities sometimes impossible to compute?
complex, many factors

2. Why is the information content of a message relative to the state of knowledge of an observer?
the more the listener knows, the less information you need to convey to reduce his uncertainty

3. Explain the relationship between entropy and redundancy.
if an encoding's efficiency matches the entropy, there is no redundancy to compress out

Lecture 37

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

it's probably english, it's probably a simple subsitution algorithm

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

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

4. How can redundancy in the source give clues to the decoding process?
if you have redundancy in the plain text that's reflected in the source text, it may mean regularities about the number of e's, for example

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,K_E),K_E),K_D).
e(p, k_e)

3. Why might a cryptanalyst want to recognize patterns in encrypted messages?
traffic analysis, it might you some clues about the scenario

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

Lecture 39

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

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?

if we have a bit string of length n, there are 2^n possibilities, and if you're just doing a linear search on that, on average when you're searching a linear space, you find the right one about halfway down, and so that means 2^(n-1) operations

3. Explain why substution and transposition are both important in ciphers.
in combination, they are very powerful

4. Explain the difference between confusion and diffusion.
confusion: transforming information in plaintext so that an interceptor cannot readily extract it;

diffusion: spreading the information from a region of plaintext widely over the ciphertext

5. Is confusion or diffusion better for encryption?
both

Lecture 40

1. What is the difference between monoalphabetic and polyalphabetic substitution?
monoalphabetic: each symbol of the plaintext is exchanged for another symbol uniformly;
polyalphabetic: different substitutions are made depending on where int he plaintext the symbol occurs

2. What is the key in a simple substitution cipher?
a table or other scheme that exhibits the mapping

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

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

5. What is the size of the keyspace in the Caesar Cipher example?
25

6. Is the Caesar Cipher algorithm strong?
no

7. What is the corresponding decryption algorithm to the Vigenere ciphertext example?
align the two texts, possibly removing spaces;
use the letter pairs to look up an encrytion in a table

Lecture 41

1. Why are there 17576 possible decryptions for the “xyy” encoding on slide 3?
26^3

2. Why is the search space for question 2 on slide 3 reduced by a factor of 27?
add the information that it's a simple substitution cipher

3. Do you think a perfect cipher is possible? Why or why not?
yes; one-time pad

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?
if you knew that it had even parity, if you work backwards you could take the cyber text and that fact and elimate half of the possible plaintext

3. Explain the key distribution problem.
if the sender and receiver already have a secure channel, wy 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

Lecture 44

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

2. Describe the difference between key distribution and key management.
key distribution: how do we convey keys to those who need them to establish secure communication;
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?
no; Ks is only used for encryption, not decryption

4. Are symmetric encryption systems or public key systems better?
keys in the two approaches have very different characteristics and are not directly comparable

Lecture 45

1. Why do you suppose most modern symmetric encryption algorithms are block ciphers?
high diffusion, immunity to tampering

2. What is the significance of malleability?
if transformations on the ciphertext produce meaningful changes in the plaintext, you are not going to have any corruption in the plaintext when you decrypt this, but maybe the meaning of the message is changed entirely

3. What is the significance of homomorphic encryption?
the homomorphic property of various cryptosystems can be used to create secure voting systems, collision-resistant hash functions, and private information retrieval schemes

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
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: 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
mixcolumns: for each column of the state, replace the column by its value multiplied by a fixed 4x4 matrix of integers

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

4. Describe the use of blocks and rounds in AES.
uses a block of 128-bits, which is modified in place in each round

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

Lecture 47

1. What is a disadvantage in using ECB mode?
identical blocks in the plaintext will yield identical blocks in the ciphertext

2. How can this flaw be fixed?
"randomize" blocks before they're encrypted

3. What are potential weaknesses of CBC?
observed changes: an attack able to observe changes to ciphertext over time will be able to spot the first block that changed;
content leak: if an attack can find two identical ciphertext blocks, he can derive a relationa nd derive information about two plaintext blocks

4. How is key stream generation different from standard block encryption
modes?
in block encryption modes (like ecb and cbc), the point is to 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 for encryption by xoring with a message stream. decryption uses the same key stream

Lecture 48

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

2. Why are one-way functions critical to public key systems?
one-way functions: easily computed, but difficult to invert without additional information

3. How do public key systems largely solve the key distribution problem?
public keys can be freely distributed, but decryption is only possible with the private 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.
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

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; the algorithm is such that {{p}_d}_e = p = {{p}_e}_d

2. Explain the role of prime numbers in RSA.
the rsa algorithm relies on teh difficulty of factoring large numbers; a plaintext block p is encrypted as (p^e)^d mod n = p; an interceptor would have to factor p^e to recover the plaintext

3. Is RSA breakable?
yes

4. Why can no one intercepting $\{M\}_{Ka}$ read the message?
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?
anyone might have a's public key

6. Why is A sure $\{M\}_{K-1}$

b

originated with B?
no one besides b has that private key

7. How can someone intercepting $\{M\}_{K_b^{-1}}$ read the message?
decrypt with b's public key

8. How can B ensure authentication as well as confidentiality when sending a message to A?
require two pairs of keys: one pair for privacy and the other pair for "signing" (authenticity)

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.
strong: m_2 != m_1

3. What is the difference between preimage resistance and second preimage resistance?
preimage resistance: given h, it is hard to find any m such that h = f(m);
second preimage resistance: given an input m_1, it is hard to find m_2 != m_1 such that f(m_1) = f(m_2)

4. What are the implications of the birthday attack on a 128 bit hash value?
you expect to find a pair of different arguments x1 and x2 with f(x1) = f(x2) after evaluating the function for about 1.25(2^64) different arguments

5. What are the implications of the birthday attack on a 160 bit hash value?
you expect to find a pair of different arguments x1 and x2 with f(x1) = f(x2) after evaluating the function for about 1.25(2^80) different arguments

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

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?
use rsa to generate a hash value

Lecture 51

1. For key exchange, if S wants to send key K to R, can S send the following

message: $\{\{K\}_{KS-1}\}_{K-1}$

R

? Why or why not?
yes

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 $\{\{\{K\}_{KS-1}\}_{K_R}\}_{K_S}$ equivalent to $\{\{K\}_{K-1}$

S

$\}_{K_R}$?
yes

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

Lecture 52

1. What would happen if g, p and $g_a$modp were known by an eavesdropper listening in on a Diffie-Hellman exchange?
nothing

2. What would happen if a were discovered by an eavesdropper listening in on a Diffie-Hellman exchange?
nothing

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

nothing