LECTURE 2

Cryptography Basics

1 Terminology

S – Sender, R – Receiver, T – Transmitter (e.g. network), O – Outsider/Interceptor, K_e – Encryption key, K_d – Decryption key

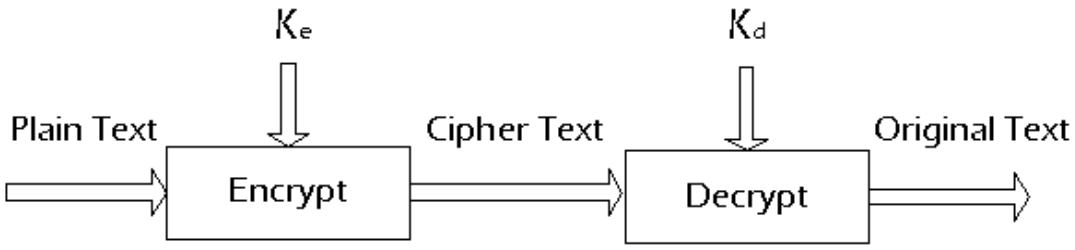

Figure 1 Encryption/Decryption

The figure above shows how a plain text is transformed to cipher text by applying a key K_e. Applying another, possibly different, key K_d, retrieves the original. When the keys used are the same, the process is known as symmetric encryption; otherwise, it is called asymmetric. In symbols, this process is shown as

$$P = D(K_d, E(K_e, P))$$

2 Substitution Ciphers

Caesar Cipher: Map $a \rightarrow D$, $b \rightarrow E$, $c \rightarrow F \ldots x \rightarrow A$, $y \rightarrow B$, $z \rightarrow C$.

To break, all you need to do is try all 25 (one is identity) possible keys.

2.1 Monoalphabetic Ciphers

Map a..z to some permutation of the alphabet. There are 26! possible keys. Trying all possibilities takes over 10^3 years. However, using letter frequencies and some facts about English, this can be broken quite easily. For example, the letter e occurs

14% of the time. If the letter e were to be mapped to x, then x would occur 14% in the cipher text. From these facts, it is easy infer that e is mapped to x.

Assume the letters in a plain text are indexed by the position they appear in the text. Then, it is likely that the letter e would fall half of the time in an index that is odd. Therefore, if two permutations are used – one for odd position and one for even position, then the peaks in letter frequencies can be even out. By using more than 2 permutations, almost uniform distribution can be achieved.

A Vigenère tableau does exactly this except instead of using arbitrary permutations it uses rotations, like the Caesar cipher. The number of permutations it uses is based on a keyword. If the keyword is juliet, then it uses 6 rotations. Every 1^{st}, 7^{th}, 13^{th} letters are mapped using a rotation jkl…xyzabc…ghi. Similarly, every 2^{nd}, 8^{th}, 14^{th} letters use the rotation uvwxyzabc…rst.

To break something encrypted using this method,

1. Find the length of the key (say n),

2. Partition the cipher text into n pieces by taking the every n^{th} character starting from 1, 2, 3 … n.

3. Decrypt each piece separately using the letter frequency information about English.

Finding the key length can be tricky. Here the method of Kasiski can be employed. This method is based on the fact that the distance between the repeated patterns in ciphered text must be a multiple of the key length.

Another method that is used to find the key length is by computing the variance between the letter frequencies in the cipher text with that in plain text. If the polyalphabetic cipher were used with a large alphabet, then the variance would be zero. If $Prob_x$ is the probability of x occurring a text of length n, then it is equal to $Freq_x/n$. The variance can be found by summing over the whole alphabet, the term $(Prob_x-1/26)^2$. This is equal to Sum over the alphabet$(Prob_x^2) - 1/26$. It can be seen from this formula that when $Prob_x$ is 1/26 (i.e. under uniform distribution), then the variance would be zero. The first term is known as the index of coincidence (IC). When monoalphabetic cipher is used, IC is 0.068. When the alphabet is of size 3, the IC is 0.047.

To decipher text that was encrypted using a substitution cipher, find the key length by using the IC values and apply the 3 steps given above.

No fixed key length

To improve on the previous methods, one could try keys with no periodic repetition. In other words, if the key were to be infinitely long random sequence of letters, and the same key is also available to the recipient, then this key can be combined with plain text, using some function such as modulo addition or exclusive OR, to get a cipher that is difficult to break. The plain text can be retrieved if the key and the combining function are known.

Since random sequences are difficult to generate, letters from phone books, and passages from well-known classics are used for keys. The recipient would have ready access to this material as well.

Example

Plain text: Hello World

Indexing the alphabet starting from 0, i.e. A(0), B(1), C(2), …, and ignoring spaces in the message

H(7) E(4) L(11) L(11) O(14) W(22) O(14) R(17) L(11) D(3)

This is combined with a sequence of 10 random numbers. Assuming random number range is between 0 and 50,

13 43 28 8 2 19 29 37 43 33

The sum mod 26 gives the indices of the cipher text:

20 21 13 19 16 15 17 2 2 10

The encrypted message is UVNTQ PRCCK

This scheme can be used with bases other than decimal as well. The binary Vernam Cipher works this way.

3 Pseudo-random numbers

A common type of generating random numbers is by using the formula:

$$R_{i+1} = (a * R_i + b) \bmod n$$

where a, b, and n are constants. The initial value R_0 is called the seed. Often, n is equal to 1+ MAXINT. The leading portion that cannot be stored in a word is ignored in intermediate calculations. If R_0 and a are relatively prime to n, then each number between 0 and n-1 are generated before the sequence repeats itself. But once the repetition starts, the whole sequence appears in the same order.

This method is not very secure. In the above equation, there are only three unknowns. Knowing R_0, R_1, R_2, and R_3 one can determine a, b and n.

Example

Assume a<n and b<n. Given

1. $6 = (a * 7 + b) \bmod n$
2. $1 = (a * 6 + b) \bmod n$
3. $0 = (a + b) \bmod n$

What are the values of a, b, and c that satisfy the above 3 equations? Write them as

1. a+b = n*I
2. 6*a+b = n*J+1
3. 7*a+b = n*K+6

for some integers I,J, and K. Eliminating b from 1 and 2, and doing other similar operations

1. 5*a mod n = 1
2. 6*a mod n = 6
3. a mod n = 5

a=5, b=3 and n=8 satisfies the above equalities.

3.1 The problem with using text from well-known books

Assume Vigenère method is used with key to be some prose from a book. In English, the letters A, E, I, N, O and T occur with 50% frequency. The chances that two of these common letters get combined are 25%. In other words, a fourth of the letters can be guessed by looking at the part of the Vigenère table containing the rows and columns corresponding to these 6 common letters. For example, if the cipher text contains the letter m, then looking at the entries for these 6 letters suggests that the corresponding plain text letter is E,I or T (combined with the key letters I, E, and T) with 25% probability. While this in itself is not enough to decrypt the entire message, it does reduce the search space for the cryptanalyst.

Example:

O N C E U P O N A T
L O C K T A R G E T

Using the standard Vigenère table, this encrypts to ZBEONPFTEM. Looking at B in the second position for example, instead of trying all possible 26 combinations, one might conclude that it is a result of combining two of the 6 most frequently occurring letter combinations, i.e. N+O. Using similar conclusions, one might be able to reduce the search space.

Combining a message with another similar message

> See you tomorrow at Time Square
> Meet you tomorrow at the capitol

The cipher text with this combination is (s+m)%26, (e+e)%26,…, (e+l)%26. Or use a rotation starting with M, rotation with e, etc.

4 Transposition Ciphers

This method works by permuting the plain text according to a set pattern. This pattern holds the key to deciphering the text.

For example, plain text of n chars can be arranged in a rectangular matrix of size ixj and reading the characters from a column major order produces cipher text. If i*j is not equal to n, then padding characters can be added at the end.

This method is said to work by diffusion whereas the previous methods use confusion.

The weakness for this method lies in the fact that English has a set digram (2-letter combinations) frequencies.

To break these ciphers,

1. Check the letter frequencies and make sure that they are the same as normal English

2. Vary the window size (the number of columns) from 2 onwards and attempt to build the plain text

3. If the resulting plain text has normal diagram frequency, the attempt was successful; otherwise, continue.

In checking for various sizes, one need not compute the whole deciphered text. Take the partially constructed text and look for “normal” digrams, i.e. common digrams should appear and uncommon ones should not appear.

Assume we transpose using 8 rows and 5 columns, for example. The 37^{th} letter in P when arranged in the matrix form would be at 8^{th} row, 2^{nd} column. Its position in D would be 16.

One way around this kind of cryptanalysis is to use two different transpositions in succession. This is an example of *product ciphers*. Doing digram analysis and guessing the mathematical relationship between the compositions can still break this cipher. Note that applying product cipher twice using a square matrix, does not do any further movement of letters.

One of the major weaknesses of transposition ciphers is that once the mathematical relationship is found, the whole scheme can be broken. Plausible mathematical relationships concerning the sizes of the matrices used can be formed by examining digrams and see how they are separated in D.

5 Fractionated Morse

Morse code is a sequence of dots and dashes with pauses to separate letters. Instead of having the same length code for each letter, the coding optimizes the total length by considering letter frequencies. The pauses between the letters can be thought of as another character. Using ternary alphabet, one can represent 27

characters. Omitting |||, we can assign one ternary code to one letter. To encrypt using this method, first the Morse code is constructed for the whole plain text. Then, a keyword (with distinct letters) is used at the beginning of the alphabet. The Morse string is broken up into 3-character long block and a letter is assigned to each block.

This encryption is almost similar to monoalphabetic substitution. But, since one letter can get mapped to different cipher letters, it is not quite that system. To break this cipher, one can use the fact that common words such as *is*, *and* and *the,* occur repeatedly.

6 Stream and Block ciphers

Advantages of stream (as plain text is fed as input, the cipher text is output, e.g. substitutions) ciphers:

- Speed of transformation
- Low error propagation – loss of one letter, one can still reconstruct the plain text

Disadvantages:

- Low diffusion – cryptanalyst can localize and try to break
- Susceptible to malicious insertions and modifications – if the interceptor notices that certain portion of the cipher text refers to an account number, then he can modify the account and send out a message that is spliced together

Advantages of block ciphers (plain text is encrypted in blocks, e.g. transpositions)

- Diffusion – account number would get broken up
- Immunity to insertions – would disturb the mathematical relationship between plain text symbols

Disadvantages:

- Slow – must wait until the whole block is available
- Error propagation – not limited to a portion

7 Characteristics of Good Ciphers

Shannon characteristics:

1. Amount of labor to encrypt is proportional to the amount of secrecy desired
2. Encryption process should be simple (may not be relevant now)
3. Errors in ciphering should not propagate

4. Size of the ciphered text should be no larger than the original message (gives the cryptanalyst more data to deduce the key)

8 Cryptanalyst scenarios

Cipher text-only – no knowledge of the key or the encryption algorithm

Known plain text – has C and P, needs to find E in C=E(P)

Chosen plain text – has infiltrated the encryption system, can insert delete records and observe the effect

Chosen cipher text – has the encryption algorithm and C, needs to find the key for future decryption