COMP/IT – 424 Homework #2

TRUE OR FALSE

T F 1. The vast majority of network based symmetric cryptographic applications make use of stream ciphers.

T F 2. The Feistel cipher structure, based on Shannon's proposal of 1945, dates back over a quarter of a century and is the structure used by many significant symmetric block ciphers currently in use.

T F 3. DES uses a 56-bit block and a 64-bit key.

T F 4. If the bit-stream generator is a key-controlled algorithm the two users only need to share the generating key and then each can produce the keystream.

T F 5. A problem with the ideal block cipher using a small block size is that it is vulnerable to a statistical analysis of the plaintext.

T F 6. Confusion seeks to make the statistical relationship between the plaintext and ciphertext as complex as possible in order to thwart attempts to deduce the key.

T F 7. All other things being equal, smaller block sizes mean greater security.

T F 8. Greater complexity in the subkey generation algorithm should lead to greater difficulty of cryptanalysis.

T F 9. Fast software encryption/decryption and ease of analysis are two considerations in the design of a Feistel cipher.

T F 10. A prime concern with DES has been its vulnerability to brute-force attack because of its relatively short key length.

T F 11. One criteria for an S-box is: "If two inputs to an S-box differ in exactly one bit, the outputs must also differ in exactly one bit. "

T F 12. The heart of a Feistel block cipher is the function F, which relies on the use of S-boxes.

T F 13. The strict avalanche criterion and the bit independence criterion appear to weaken the effectiveness of the confusion function.

T F 14. An advantage of key-dependent S-boxes is that because they are not fixed, it is impossible to analyze the S-boxes ahead of time to look for weaknesses.

T F 15. The key schedule algorithm is more popular and has received more attention than S-box design.

MULTIPLE CHOICE

1. DES exhibits the classic _____ block cipher structure, which consists of a number of identical rounds of processing.

   A) Feistel B) SAC

   C) Shannon D) Rendell

2. A sequence of plaintext elements is replaced by a _____ of that sequence which means that no elements are added, deleted or replaced in the sequence, but rather the order in which the elements appear in the sequence is changed.

   A) permutation B) diffusion

   C) stream D) substitution

3. A _____ cipher is one that encrypts a digital data stream one bit or one byte at a time.

   A) product B) block

   C) key D) stream

4. The vast majority of network-based symmetric cryptographic applications make use of _____ ciphers.

   A) linear B) block

   C) permutation D) stream

5. A _____ cipher is one in which a block of plaintext is treated as a whole and used to produce a ciphertext block of equal length.

   A) bit B) product

   C) stream D) block

6. _____ is when each plaintext element or group of elements is uniquely replaced by a corresponding ciphertext element or group of elements.

A) Substitution B) Diffusion

C) Streaming D) Permutation

7. Key sizes of _____ or less are now considered to be inadequate.

A) 128 bits B) 32 bits

C) 16 bits D) 64 bits

8. Feistel proposed that we can approximate the ideal block cipher by utilizing the concept of a _____ cipher, which is the execution of two or more simple ciphers in sequence in such a way that the final result or product is cryptographically stronger than any of the component ciphers.

A) linear B) permutation

C) differential D) product

9. The criteria used in the design of the _____ focused on the design of the S-boxes and on the P function that takes the output of the S-boxes.

A) Avalanche Attack B) Data Encryption Standard

C) Product Cipher D) Substitution Key

10. The greater the number of rounds, the _____ it is to perform cryptanalysis.

A) easier B) less difficult

C) equally difficult D) harder

11. The function F provides the element of _____ in a Feistel cipher.

A) clarification B) alignment

C) confusion D) stability

12. One of the most intense areas of research in the field of symmetric block ciphers is _____ design.

A) S-box B) F-box

C) E-box D) D-box

13. Mister and Adams proposed that all linear combinations of S-box columns should be _____ which are a special class of Boolean functions that are highly nonlinear according to certain mathematical criteria.

A) horizontal functions B) angular functions

C) bent functions D) vertical functions

14. The Nyberg approach that is more or less a manual approach with only simple mathematics to support it is _____ .

A) human-made B) random

C) math-made D) random with testing

15. Allowing for the maximum number of possible encryption mappings from the plaintext block is referred to by Feistel as the _____ .

A) ideal substitution cipher B) round function

C) ideal block cipher D) diffusion cipher

SHORT ANSWER

1. A block cipher is an encryption/decryption scheme in which a block of plaintext is treated as a whole and used to produce a ciphertext block of equal length.

2. Confusion seeks to make the relationship between the statistics of the ciphertext and the value of the encryption key as complex as possible so that even if the attacker can get some handle on the statistics of the ciphertext, the way in which the key was used to produce that ciphertext is so complex it is difficult to deduce the key.

3. Many block ciphers have a Feistel structure which consists of a number of identical rounds of processing and in each round a substitution is performed

on one half of the data being processed, followed by a permutation that interchanges the two halves.

4. Feistel's is a practical application of a proposal by Claude Shannon to develop a product cipher that alternates confusion and diffusion functions.

5. The guaranteed avalanche (GA) criterion is defined as: "An S-box satisfies GA of order y if, for a 1-bit input change, at least y output bits change."

6. In diffusion the statistical structure of the plaintext is dissipated into long-range statistics of the ciphertext. This is achieved by having each plaintext digit affect the value of many ciphertext digits.

7. The most widely used encryption scheme is based on the DES adopted in 1977 by the National Bureau of Standards as Federal Information Processing Standard 46.

8. A change in one bit of the plaintext or one bit of the key should produce a change in many bits of the ciphertext. This is referred to as the avalanche effect.

9. Two areas of concern regarding the level of security provided by DES are the nature of the algorithm and the key size .

10. A timing attack exploits the fact that an encryption or decryption algorithm often takes slightly different amounts of time on different inputs.

11. The bit independence criterion states that output bits j and k should change independently when any single input bit i is inverted for all i, j and k.

12. The Feistel cipher structure, which dates back over a quarter century and which, in turn, is based on Shannon's proposal of 1945, is the structure used by many significant symmetric block ciphers currently in use.

13. The cryptographic strength of a Feistel cipher derives from three aspects of the design: the function F, the key schedule algorithm, and the number of rounds.

14. The strict avalanche criterion states that any output bit j of an S-box should change with probability 1/2 when any single input bit i is inverted for all i,j.

Two alternatives to DES are AES and triple DE

COMP/IT – 424 Homework #2

Problems

1. Consider a substitution cipher where 52 symbols were used instead of 26. In particular, each symbol in the cipher text is for either a lowercase English letter, or an uppercase English letter. (For example, let E be the encryption function then we could have

   E(S) = p and E(s)=m

   Such a modification augments the key space to 52! Does this provide added security compared to a standard substitution cipher? Why or why not?

This does not add much security to the system at all. Capital letters usually appear only at the beginning of words at the beginning of sentences. Thus, the frequencies of capital letters are quite small in English text. You could simply consider this while using frequency analysis. Simply put, disregard all the characters of very small frequencies and concentrate on solving for the characters with the highest frequencies, which will still be the same lowercase letters. Once these are solved for, there will be enough recovered plaintext to deduce most if not all of the capital letters in the message.

2. We consider the one-time pad with messages and key-streams both binary sequences. Suppose that the system is used erroneously, so that two messages have been encrypted using the same key. What information can an adversary that hears the two ciphertexts deduce about the plaintexts?

The described situation is $C1 = K \oplus M1$

$C2 = K \oplus M2$

From this we get

$C1 \oplus C2 = (K \oplus M1) \oplus (K \oplus M1) = M1 \oplus M2$

i.e. the Adversary can identify exactly in which bit positions the two messages differ.

3. Assuming you can do 2^{20} encryptions per second and the key size is 40 bits, how long would a brute force attack take? Give a scenario where this would be practical and another where it wouldn't. What happens if you double the key size?

The key space has 2^{40} elements, so brute force would take 2^{20} seconds, which is about 12 days (half that time if you consider that on average trying half the key space would yield success). This would be practical if the message revealed the location of enemy missiles in a cold-war situation. It would be impractical if the message's useful life was very short, for example if it was a few frames in a pay-per-view sports video.

Doubling the key size would make the brute force decryption time 2^{60} seconds, which is about 3.8×10^{16} years. There is no scenario in which this would be practical.