Fall 1996 EE 578/CS 578, WPI Section Prof. Christof Paar

Midterm Exam

October 21, 1996

Name: ____________________________

1. What is Kerckhoff's principle? Why is it used in cryptography?

2. A message is double encrypted with

$$y = e_{k1}(e_{k2}(x)), \tag{1}$$

where e_{k1} and e_{k2} are two affine ciphers with the parameters $a_1 = 25, b_1 = 20$ and $a_2 = 17, b_2 = 21$.

(a) Find the parameters $c, d \in Z_{26}$ such that

$$x = c\,y + d \bmod 26$$

decrypts a message encrypted with (1).

(b) Decrypt the message:
`BJWVMTDV`
using the attached mapping from letters to numbers.

(c) Why is double encryption with the affine cipher not effective?

3. We consider the stop-and-go generator. The first LFSR is of degree $m_1 = 2$ and the feedback coefficients are given by $x^2 + x + 1$, the second LFSR is of degree $m_2 = 3$ and has the feedback coefficients $x^3 + x + 1$,

(a) Your task is to choose the third LFSR. You have to choose between:

- $m_3 = 4, \;\; x^4 + x + 1$
- $m_3 = 7, \;\; x^7 + x + 1$
- $m_3 = 9, \;\; x^9 + x + 1$

where each of the LFSRs has maximum period. Which LFSR results in the longest sequence length for the stop-and-go generator?

(b) Assume the initial vector $(z_0 = 1, 0)$ for the first LFSR, and $(z_0 = 1, 0, 0)$ for the second LFSR. Use you answer from (3a) with $(z_0 = 1, 0, \ldots, 0)$ for the third LFSR. Draw the circuit diagram and compute the first five bits of the key stream.

4. Attached is a description of the DES key schedule. Assume a 64 bit key:

   ```
   K = 1100 0001 0000 0001 0000 0001 ...  0000 0001
   ```

   The leftmost bit is bit number one. Compute the sub key K_{16}. (Note that bits $8, 16, 24, \ldots, 64$ are parity bits which are not passed through PC-1.)

5. There are relatively new private-key algorithms with variable key length. Your task is to determine the key length such that a certain long term security against an exhaustive key search attack is provided.

   We assume that one encryption (or key test) can be performed in 10^{-7} s with today's technology, and that 1 million encryption chips are used in parallel in our machine. Furthermore, assume that Moore's law holds, according to which computational power doubles every 18 months.

   (a) How many key bits are required so that a brute force attack with today's technology takes a least one hour on average?

   (b) What is the minimum number of key bits so that a brute force attack 30 years from now takes at least one hour on average.

6. Given are the following parameters of the RSA cryptosystem: $p = 97, q = 101, b = 1003$. You receive the ciphertext $y = 2709$. Compute the cleartext.

7. Many practical cryptosystems utilize private-key algorithms as well as public-key ones. What is the advantage of using such hybrid systems?