Mathematics 360 **Homework (due Oct 16)** A. Hulpke

29) Let $p = 31$ (which is prime). Then $a = 3$ is a primitive root modulo p. (You don't need to show this). Determine the orders of the powers a^e for $1 \le e \le 30$. (**Hint:** Problem 19)

30) Let V be the row space of the matrix

$$\begin{pmatrix} 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 \end{pmatrix}$$

over the field $\mathbb{F}_2 = GF(2) = \mathbb{Z}/2\mathbb{Z}$ with 2 elements. Determine the dimension of V.

31) Consider the following S-box (which is box S_1 in the DES). It takes as input a 6 bit sequence, the outermost 2 bits determine the row, the middle 4 the column and the resulting sequence is returned. (For example, sequence 101010 has outer bits 10 and thus is entry 0101 in row 3, so returns 0110.) Show that the function $\mathbb{F}_2^6 \to \mathbb{F}_2^4$ implemented by this S-box is not linear.

	Middle 4 bits															
Out	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
00	1110	0100	1101	0001	0010	1111	1011	1000	0011	1010	0110	1100	0101	1001	0000	0111
01	0000	1111	0111	0100	1110	0010	1101	0001	1010	0110	1100	1011	1001	0101	0011	1000
10	0100	0001	1110	1000	1101	0110	0010	1011	1111	1100	1001	0111	0011	1010	0101	0000
11	1111	1100	1000	0010	0100	1001	0001	0111	0101	1011	0011	1110	1010	0000	0110	1101

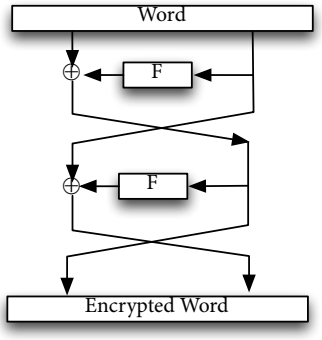
32) Explain why (beyond the issue of composition of linear functions as discussed in the lecture) an encryption scheme should not be a linear function. (**Hint:** What would happen if you know a number of linear independed messages as well as their encrypts?)

33)

Take a baby version of DES that operates on 8 bits in two rounds. In each round the function F applied to the right 4 bits consists of

1. Expand the sequence $abcd$ to $cabcda$.
2. Add the key K_i modulo 2 (XOR, $\oplus$).
3. Reduce the result back to 4 bit with the S-box given in problem 32.

The result of $F(\text{right})$ then is added to the left 4 bits modulo 2.



We are using the encryption keys K_1 = 101010 and K_2 = 110011.
a) Encrypt the word 11100110 with these keys. Show the intermediate results.
b) Verify that the encrypted word decripts correctly.

34) Suppose you wish to obtain a decimal digit at random. Which of the following methods would be suitable, and why (considering randomness, not repeatability)?

a) Open a telephone directory to a random place by sticking your finger in it somewhere, and use the units digit of the first number found on the selected page.

b) Same as (a), but use the units digit of the page number.

c) Roll a die that is in the shape of a regular icosahedron, whose twenty faces have been labeled with the digits 0, 0, 1, 1, ... , 9, 9. Use the digit that appears on top, when the die comes to rest. (A felt-covered table with a hard surface is recommended for rolling dice.)

d) Expose a geiger counter to a source of radioactivity for one minute (shielding yourself) and use the units digit of the resulting count. Assume that the geiger counter displays the number of counts in decimal notation, and that the count is initially zero.

e) Glance at your wristwatch; and if the position of the second-hand is between $6n$ and $6(n+1)$ seconds, choose the digit n.

f) Ask a friend to think of a random digit, and use the digit he names.

g) Ask an enemy to think of a random digit, and use the digit he names.

h) Assume that 10 horses are entered in a race and that you know nothing whatever about their qualifications. Assign to these horses the digits 0..9 in arbitrary fashion, and after the race use the winner's digit.