Dr. A. Betten Fall 2005

M360 Mathematics of Information Security

practice exam 10/28/05

not graded!

Exercise # 1 (points)

a) What is $X^4 + X^3 + X + 1$ divided by $X^2 + X + 1$ over $\mathbb{Z}_2$?

b) What is $X^6 + X^3 + X + 1$ divided by $X^2 + X + 1$ over $\mathbb{Z}_2$?

c) What is $X^4 + 2X^2 + X + 2$ divided by $X^2 + 2$ over $\mathbb{Z}_3$?

Exercise # 2 (points)

a) What is $X^4 + X^3 + X + 1$ times $X^2 + X + 1$ modulo $X^4 + X^3 + 1$ over $\mathbb{Z}_2$?

b) What is $X^4 + 2X^2 + X + 2$ times $X^2 + 2$ modulo $X^3 + 2$ over $\mathbb{Z}_3$?

Exercise # 3 (points)

Compute the gcd of the two polynomials over $\mathbb{Z}_2$ $p(X) = X^3 + X^2 + 1$ and $q(X) = X^4 + X$ and express it as a linear combination of the two.

Exercise # 4 (points)

Show that $X^2 + 1$ is irreducible in $\mathbb{Z}_3[X]$. Find the multiplicative inverse of $1 + 2X$ in $\mathbb{Z}_3[X]$ mod $X^2 + 1$.

Exercise # 5 (points)

a) Find all four solutions to $x^2 \equiv 133 \bmod 143$

b) Find all two solutions to $x^2 \equiv 77 \bmod 143$

Exercise # 6 (points)

A group of people are arranging themselves for a parade. If they line up three to a row, one person is left over. If they line up four to a row, two people are left over., and if they line up five to a row, three people are left over. What is the smallest possible number of people? What is the next smallest number?

Exercise # 7 (points)

Find the last two digits of 999^{666}.

Exercise # 8 (points)

a) List the two differences between DES *decryption* and DES *encryption*.

b) Decrypt the simple-DES ciphertext

AQMn

using the key 011010011. Use the table below to code symbols to 6-bit integers. Use the simple-DES machines on the attached sheets (note that you have to change something for decryption). The S-boxes are:

$$S_1 : \begin{bmatrix} 101 & 010 & 001 & 110 & 011 & 100 & 111 & 000 \\ 001 & 100 & 110 & 010 & 000 & 111 & 101 & 011 \end{bmatrix}$$

$$S_2 : \begin{bmatrix} 100 & 000 & 110 & 101 & 111 & 001 & 011 & 010 \\ 101 & 011 & 000 & 111 & 110 & 010 & 001 & 100 \end{bmatrix}$$

	dec.	binary
a	0	000000
b	1	000001
c	2	000010
d	3	000011
e	4	000100
f	5	000101
g	6	000110
h	7	000111
i	8	001000
j	9	001001
k	10	001010
l	11	001011
m	12	001100
n	13	001101
o	14	001110
p	15	001111

	dec.	binary
q	16	010000
r	17	010001
s	18	010010
t	19	010011
u	20	010100
v	21	010101
w	22	010110
x	23	010111
y	24	011000
z	25	011001
' '	26	011010
0	27	011011
1	28	011100
2	29	011101
3	30	011110
4	31	011111

	dec.	binary
A	32	100000
B	33	100001
C	34	100010
D	35	100011
E	36	100100
F	37	100101
G	38	100110
H	39	100111
I	40	101000
J	41	101001
K	42	101010
L	43	101011
M	44	101100
N	45	101101
O	46	101110
P	47	101111

	dec.	binary
Q	48	110000
R	49	110001
S	50	110010
T	51	110011
U	52	110100
V	53	110101
W	54	110110
X	55	110111
Y	56	111000
Z	57	111001
'.'	58	111010
5	59	111011
6	60	111100
7	61	111101
8	62	111110
9	63	111111