Problem 1)

b) Calculate $-99 \bmod 1001$

$$-\frac{99}{1001} = -0.0989$$

$$q = -1$$

$$r = a - b * q = -99 - 1001 * (-1) = 902$$

c) Calculate $232 + 22 \cdot 77 - 18^3 \bmod 8$

$$(232 + 22 * 77 - 18^3) mod\ 8 =$$

$$(232\ mod\ 8 + (22 * 77) mod\ 8 - 18^3 mod\ 8) mod\ 8$$

$$232\ mod\ 8 = 0$$

$$22 * 77\ mod\ 8 = (22\ mod\ 8 * 77\ mod\ 8) mod\ 8 = 6$$

$$18^3\ mod\ 8 = 0$$

$$(232 + 22 * 77 - 18^3) mod\ 8 = 6$$

d) Determine if $55 \equiv 77 \pmod{12}$

$$55 \equiv 77 \pmod{12}$$

$$55\ mod\ 12 = 7$$

$$77\ mod\ 12 = 5$$

$$7 \neq 5$$

So $55 \equiv 77 \pmod{12}$ is not true!

Problem 2)

a) Write the multiplication table of the elements of Z_{12}, excluding the 0 element.

$$Z_{12} = \{0,1,2,3,4,5,6,7,8,9,10,11\}$$

X	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**
1	**1**	2	3	4	5	6	7	8	9	10	11

2	2	4	6	8	10	0	2	4	6	8	10
3	3	6	9	0	3	6	9	0	3	6	9
4	4	8	0	4	8	0	4	8	0	4	8
5	5	10	3	8	**1**	6	11	4	9	2	7
6	6	0	6	0	6	0	6	0	6	0	6
7	7	2	9	4	11	6	**1**	8	3	10	5
8	8	4	0	8	4	0	8	4	0	8	4
9	9	6	3	0	9	6	3	0	9	6	3
10	10	8	6	4	2	0	10	8	6	4	2
11	11	10	9	8	7	6	5	4	3	2	**1**

b) Which integers have a multiplicative inverse modulo 12?

S = {1, 5, 7, 11}

c) Do the same for Z_{11}. Which numbers have mult.inverse mod 11?

X	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
1	1	2	3	4	5	6	7	8	9	10
2	2	4	6	8	10	1	3	5	7	9
3	3	6	9	1	4	7	10	2	5	8
4	4	8	1	5	9	2	6	10	3	7
5	5	10	4	9	3	8	2	7	1	6
6	6	1	7	2	8	3	9	4	10	5
7	7	3	10	6	2	9	5	1	8	4
8	8	5	2	10	7	4	1	9	6	3
9	9	7	5	3	1	10	8	6	4	2
10	10	9	8	7	6	5	4	3	2	1

S = {1,2,3,4,5,6,7,8,9,10}

11 is prime so all the numbers have mult.invese mod 11.

d) Find the multiplicative inverse to 11 modulo 29, by trial and error, ie. just try different values.

$$11 * x \equiv 1 \, mod \, 29$$

X	11*x	Mod 29
1	11	11
2	22	22
3	33	4
4	44	15

5	55	26
6	66	8
7	77	19
8	88	1

The multiplicative inverse to 11 mod 29 is 8.

e) Formulate a condition for a to have a multiplicative inverse modulo n.

Hint: It involves the factorizations of a and n.

An integer a has a multiplicative inverse to n if gcd(a, n) = 1.

This means if a and n don't share any common factors other than 1.

Problem 3)

$e_k(x)=(3 \cdot x+11) \bmod 26$

a) Write e_k as a permutation, i.e. the sequence of letters we get when encrypting a, b, c etc.

a -> L
b -> O
c -> R
d -> U
e -> X
f -> A
g -> D
h -> G
i -> J
j -> M
k -> P
l -> S
m -> V
n -> Y
o -> B
p -> E
q -> H
r -> K
s -> N
t -> Q

u -> T
v -> W
w -> Z
x -> C
y -> F
z -> I

b) Use e_k to encrypt the message m = 'alice'

alice->LSJRX

c) Find the inverse of e_k as a

- permutation as in part a)
- as a formula $d_k(y) = ay + b \pmod{26}$ (the decryption) where you have to determine a and b.
- Hint: Invert the formula for e_k, where you need to use a multiplicative inverse.

$e_k(x)=(3 \cdot x+11) \bmod 26$

- ⇨ $d_k(e_{k(x)}) \equiv x \bmod 26$
- ⇨ $d_k(x) = a^{-1}(x-b) mod\ 26\ where\ a = 3, b = 11$
- ⇨ $3 * x \equiv 1 \bmod 26$
- ⇨ $3 * 9 = 27\ mod\ 26 \equiv 1$
- ⇨ $d_k(x) = 9 * (x - 11)\ mod\ 26$
- ⇨ $d_k(x) = (9 * x - 99) mod\ 26$
- ⇨ $d_k(x) = 9 * x - 21\ mod\ 26$

d) Use the inverse d to decrypt c = RBKKXRQ

Decrypted = correct

e) How secure is this cipher, compared to a rotation cipher? Consider both brute force and known plaintext attacks.

Rotation ciphers only normally have 26 keys, meaning you could crack the cipher in a maximum of 26 tries. Generally, you could say that you can crack a rotation cipher with X keys, in X tries.

Affine ciphers have more keys $\varphi(x) \cdot x$, this means that you must try a lot more combinations to get the right combination of a and b to crack the cipher.

The Affine cipher is still weak in modern standards. You could still easily crack the key with a computer.

f)

Affine key: k = (a,b)

$a \in \mathbb{Z}_{26}^{*}$ (must be coprime with 26): 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25 → **12**

$b \in \mathbb{Z}_{26} \rightarrow 26$ choices

$12 \cdot 26 = 312$

Problem 4)
I've not found any English version of the cipher. This is what I found.
Key: (a=15, b=4)
Which deciphers to: NOEN GANGER ER DET ALL RIGHT

Problem 5)

By using decode.fr I found out that the most likely character used for space was "D", so I swapped the "D" and ".", and that cracked the cipher.

Decrypted text:

MONOALPHABETIC SUBSTITUTION CAN IN GENERAL EASILY BE BROKEN USING FREQUENCY ANALYSIS THIS ONLY WORKS WELL IF THE PLAINTEXT IS LONG ENOUGH AND IS NOT TOO DIFFERENT FROM NORMAL TEXT ONE SHOULD ALSO KNOW WHAT LANGUAGE THE PLAINTEXT IS WRITTEN IN AS THE FREQUENCIES OF LETTERS VARY FROM LANGUAGE TO LANGUAGE SOME TEXTS ARE HARDER TO BREAK THAN OTHERS AN EXAMPLE IS THE SENTENCE THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG THIS SENTENCE CONTAINS EVERY LETTER OF THE ALPHABET NOT HELPING THE CRYPTANALYST GOOD LUCK