Questions 1

(a) $28 = 7 \cdot 4 = 7 \cdot 2^2$

$\varphi(28) = 6 \cdot 1 \cdot 2 = 12$

$31^{120} \equiv 1 \ [28]$

$31^{123} \equiv 31^3 \ [28]$

$31 \equiv 3 \ [28]$
$31^3 \equiv 27 \ [28]$

So $31^{123} \equiv 27 \ [28]$
$\equiv -1 \ [28]$

(b) $7-9+4-3+2 = 3-9+7$

$= 1$

$1 \equiv 1 [11]$

$10 \equiv -1 [11]$ etc.

$100 \equiv 1 [11]$

$23497 = 7 + 10 \cdot 9 + 100 \cdot 4 + \dots$

Question 2

			$\tilde{v}$	$\tilde{u}$
$\gcd(a,b)$	$a = bq + r$	q	u	v
$\gcd(70,51)$	$70 = 51 \cdot 1 + 19$	1		
$\gcd(51,19)$	$51 = 19 \cdot 2 + 13$	2		
$\gcd(19,13)$	$19 = 13 \cdot 1 + 6$	1		
$\gcd(13,6)$	$13 = 6 \cdot 2 + 1$	2		
$\gcd(6,1)$	$6 = 1 \cdot 6 + 0$	6	0	1
$\gcd(1,0)$	$1 = 0 \cdot 0 + 1$	0	1	0

on cherche $1 = 1 \cdot u + 0 \cdot v$

$$1 = 51 \cdot 3 + 19 \cdot (-8)$$

$$= 153 + -\overset{7}{8}2$$

$$= 153 - 152$$

$$= 1$$

Question 3

01

10011 = k

k' = (1, 1, 1, 0, 1)

to cipher : 01001

10100

→ one time pad

→ on peut avoir toutes les clefs possibles

Question 4

We want to find the inverse of

$[10]_{56}$

56
112
168
224
280

560 - 56 = 504
- 56 = 448
= 392

50

10 · 49 = 490
- 38
= 452

- 56 = 434

10 · 41 = 410
- 38
372

$$\begin{array}{r} 180 \\ -\ 38 \\ \hline 142 \end{array}$$

Question 5

$24x = [4]_{45}$

$24 \cdot 0 \equiv 0 \ [45]$
$24 \cdot 1 \equiv 24 \ [45]$
$24 \cdot 2 \equiv 3 \ [45]$
$24 \cdot 3 \equiv 27 \ [45]$
$24 \cdot 4 \equiv 6 \ [45]$
$24 \cdot 5 \equiv 30 \ [45]$
$24 \cdot 6 \equiv 9 \ [45]$
$24 \cdot 7 \equiv 33 \ [45]$

12
36
15
39
18
42
↳ va se répéter car $[45]_{45} = [0]_{45}$

1
72

1
96

2
120

45
90
135
180

$24 \cdot q = -(+4)$

↓

on veut que le pgcd soit 4 ou 9

$\Rightarrow q$ soit pair 6, 1

$1 \equiv$

11

16

21

26

31

36

41

$$[24]_{45}\, x = [4]_{45}$$

$$\Rightarrow [6]_{45}\,[4]_{45}\, x = [4]_{45}$$

$$\Rightarrow [3]_{45}\,[2]_{45}\,[4]_{45}\, x = [4]_{45}$$

$$\Rightarrow [3]_{45}\,[2]_{45}\, x = [1]_{45}$$

$$\Rightarrow [6]_{45}\, x = [1]_{45}$$

$\Rightarrow$ mais x n'est pas inversible modulo 45, donc il n'y a pas de solution x