Assignment 8

1.

a:

Als 7 vrienden besluiten te samenzweren, hebben ze al 128-16 = 112 bits van de key. De laatste zestien bits van de key moeten ze nog raden. Het laatste stuk heeft: 2^{16} = 65536 mogelijke combinaties. Dit is er van uitgaande dat ze weten op welke plek elk stukje key moet. Als ze ook niet weten in welke volgorde ze de stukjes key moeten zetten dan moeten ze dat ook nog proberen, er zijn 8 stukjes key dus 8 * 7 * 6 * 5 * 4 * 3 * 2 * 1 mogelijke combinaties.

Als we alles bij elkaar optellen zijn er dus:

8 * 7 * 6 * 5 * 4 * 3 * 2 * 1 * 65536 = 2642411520 mogelijkheden die ze moeten proberen.

2

a:

1000 mod 7 = 6

Als je vanaf Vrijdag, zes dagen vooruit rekent dan kom je uit op een Donderdag.

b:

2^1 = 2

2^2= 4

2^3= 8

2^4= 16

2^5= 32

2^6= 64

2^7= 128

…

De rij laatste getallen (2 – 4 – 8 – 6) herhaalt zich elke keer.

1893 mod 4 = 1 dus het laatste getal is een 2.

3

a:

Z_{10}	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9
2	0	2	4	6	8	0	2	4	6	8
3	0	3	6	9	2	5	8	1	4	7
4	0	4	8	2	6	0	4	8	2	6
5	0	5	0	5	0	5	0	5	0	5
6	0	6	2	8	4	0	6	2	8	4
7	0	7	4	1	8	5	2	9	6	3
8	0	8	6	4	2	0	8	6	4	2
9	0	9	8	7	6	5	4	3	2	1

b:

?

c:

?

4

A = 4 D = 3
B = 2 E = 3
C = 4

5

a:

75 $= 3 * 5^2$
210 $= 2 * 3 * 5 * 7$

GCD $= 3 * 5 = 15$

b:

66 $= 2^1 * 3^1 * 5^0 * 7^0 * 11^1$
135 $= 2^0 * 3^3 * 5^1 * 7^0 * 11^0$
GCD $= 2^0 * 3^1 * 5^0 * 7^0 * 11^0$

c:

Per priemgetal vergelijken we bij de twee getallen in de gcd(x, y) en nemen we de kleinste macht dus als:

$X = 2^2 \ldots$
$Y = 2^3 \ldots$

Dan:

$Gcd(x, y) = 2^2 * \ldots$

Dit doen we per 'gefactoriseerd' priemgetal.
Voorbeeld:

$X = 2^3 * 3^0 * 5^7 \ldots$
$Y = 2^0 * 3^0 * 5^3 \ldots$

$Gcd(x, y) = 2^0 * 3^0 * 5^3 \ldots$
Want:
$0 < 3$,
$0 = 0$,
$3 < 7$