Assignment 13

1.

a.

$g^a = 93 = 10^{317} \bmod 1021$

b.

$g^b \bmod 1021 = 491$

$10^b \bmod 1021 = 491$

Ingevuld in wolframAlpha → b = 1032

c.

a = 317

b = 1032

$g^b = 491$

$491^a \bmod 1021 = 491^{317} \bmod 1021 = 93^b \bmod 1021 = 93^{1032} \bmod 1021 = 71$

d.

i:

A → E: p = 1021, g = 10, $g^a = 93$

E → B: p = 1021, g = 10, $g^{eB} = 603$

B → E: $g^b = 491$

E → A: $g^{eA} = 129$

ii:

$K_{AE} = 93^{37} \bmod 1021 = 102 = 129^{317} \bmod 1021$

$K_{BE} = 491^{404} \bmod 1021 = 707 = 603^{1032} \bmod 1021$

2.

a.

p = 31

g = 3

a = 17

$g^a \bmod p = 3^{17} \bmod 31 = 22 = A$

	r	e	m	e	m	b	e	r
Mapping	18	5	13	5	13	2	5	18
r	3	6	9	12	15	18	21	24

A^r	15	8	27	2	30	16	23	4
c1	27	16	29	8	30	4	15	2
c2	22	9	10	10	18	1	22	10
Decryption								
c_1^{-a}	29	4	23	16	30	2	27	8
m	18	5	13	5	13	2	5	18

b & c:

3.

a.

$A = 3^{21} = 17$

b.

i: gcd(28, 5) = 1

ii: s1 = gr mod p = 3^5 mod 29 = 11

iii:

r^{-1}

28 = 5 * 5 + 3

5 = 1 * 3 + 2

3 = 1 * 2 + 1

1 = 3 – 2

1 = 3 - (5 – 3)

1 = 3 – 5 + 3

1 = -5 + 2 * 3

1 = -5 + 2 * (28 – 5 * 5)

1 = 2 * 28 – 11 * 5

$r^{-1} = 17$

iv: $s_2 = (15 – 21 * 11) * 17 \mod 28 = 24$

c.

i: Ja!

ii: $v = 11^{24} * 17^{11} \mod 29 = 26$

iii: 3^{15} mod 29 = 26, Ja dat klopt!