MATH 178 Homework #5

Tamir Enkhjargal

April 2019

FF

1.

i)

2^1	2^2	2^3	2^4	2^5	2^6	2^7	2^8	2^9	2^{10}	2^{11}	2^{12}
2	4	8	3	6	12	11	9	5	10	7	1

Table 1: The set 2^i that generates $\mathbb{F}_{13}^*$

ii)

i	$2^i = b$	r
1	2	12
2	4	6
3	8	4
4	3	3
5	6	12
6	12	11
7	11	12
8	9	3
9	5	4
10	10	6
11	7	12
12	1	1

Table 2: The set of numbers r where $2^r = 1(\text{mod}13)$

iii) $(2^i)^r = 1(\text{mod}13)$ and $\log_2(i) = r$

iv)

$$3 \cdot 12(\mathrm{mod} 13) = 10 \tag{1}$$
$$\log_2(3) = 4 \tag{2}$$
$$\log_2(12) = 1 \tag{3}$$
$$\log_2(3 * 12) = 6 \tag{4}$$

$$9 \cdot 10(\mathrm{mod} 13) = 12 \tag{5}$$
$$\log_2(9) = 3 \tag{6}$$
$$\log_2(10) = 6 \tag{7}$$
$$\log_2(9 * 10) = 1 \tag{8}$$

$$11 \cdot 5(\mathrm{mod} 13) = 3 \tag{9}$$
$$\log_2(11) = 12 \tag{10}$$
$$\log_2(5) = 4 \tag{11}$$
$$\log_2(11 * 5) = 3 \tag{12}$$

$$\log_2(ab) = \log(a) + \log(b)(\mathrm{mod} p - 1) \tag{13}$$

2.

i)

3^1	3^2	3^3	3^4	3^5	3^6	3^7	3^8	3^9	3^{10}	3^{11}	3^{12}	3^{13}	3^{14}	3^{15}	3^{16}
3	9	10	13	5	15	11	16	14	8	7	4	12	2	6	1

Table 3: The set 3^i that generates $\mathbb{F}_{17}^*$

ii) The smallest power of i that gives 2 is 14.

iii) The power of r of 2 that gives me 1 is 12.

LM

3.

i) $a =$ `nextprime(2^50)` $= 1125899906842679$
$b =$ `nextprime(3^50)` $= 717897987691852588770277$
`m = 11^27 = 13109994191499930367061460371`
`Mod(a,m)^b = 4860801571852662355081569 12`

ii) `Mod(a,m)^-1 = 11055863773943407120032220 35`

iii) `d = lift(c)`
`f = (d*a)-1)/m = 94948905478684`

iv) `gcd(m,8689142)=11`

v) No writeup.

vi) Decrypted Message: `That is all`

SC

1.

2 generates $\mathbb{F}_{83}^*$, and 5 generates $\mathbb{F}_{2*83+1}^*$. Secret key $k = 7$

Modular arithmetic	$= \mathrm{S}_i$	mod 2	$= \mathrm{K}_i$
$5^7 \bmod 167$	$= 136$	mod 2	$= 0$
$136^2 \bmod 167$	$= 126$	mod 2	$= 0$
$126^2 \bmod 167$	$= 11$	mod 2	$= 1$
$11^2 \bmod 167$	$= 121$	mod 2	$= 1$
$121^2 \bmod 167$	$= 112$	mod 2	$= 0$
$112^2 \bmod 167$	$= 19$	mod 2	$= 1$
$19^2 \bmod 167$	$= 27$	mod 2	$= 1$
$27^2 \bmod 167$	$= 61$	mod 2	$= 1$
$61^2 \bmod 167$	$= 47$	mod 2	$= 1$
$47^2 \bmod 167$	$= 38$	mod 2	$= 0$
$38^2 \bmod 167$	$= 108$	mod 2	$= 0$
$108^2 \bmod 167$	$= 141$	mod 2	$= 1$
$141^2 \bmod 167$	$= 8$	mod 2	$= 0$
$8^2 \bmod 167$	$= 64$	mod 2	$= 0$
$64^2 \bmod 167$	$= 88$	mod 2	$= 0$
$88^2 \bmod 167$	$= 62$	mod 2	$= 0$

Our keystream is then `0011 0111 1001 0000`. XORing the ciphertext with the keystream gets us:

Ciphertext	0110	1101	1111	0111
Keystream	0011	0111	1001	0000
Plaintext	0101	1010	0110	0111

Plaintext (in binary) = `01011010 01100111`
Plaintext (in ASCII) = `Zg`