8

Cryptography I
Homework sheet 13

Erwin van Duijnhoven
0719562

Rick Staals
0716184

January 8, 2014

Question 1

Let $n = 263$. Run the Fermat test for $k = 3$ with $a = 2, 3$, and 5.

2/2

Solution:

$$\gcd(263, 2) = 1 \quad \checkmark$$
$$2^{262} \equiv 1 \mod 263 \quad \checkmark$$

$$\gcd(263, 3) = 1 \quad \checkmark$$
$$3^{262} \equiv 1 \mod 263 \quad \checkmark$$

$$\gcd(263, 5) = 1 \quad \checkmark$$
$$5^{262} \equiv 1 \mod 263 \quad \checkmark$$

Therefore 263 is probably prime of Carmichel.

Question 2

Let $n = 263$. Run the Miller-Rabin test for $k = 3$ with $a = 2, 3$, and 5.

2/2

Solution:

$$\gcd(263, 2) = 1 \quad \checkmark$$
$$2^{131} \equiv 1 \mod 263 \quad \checkmark$$

$$\gcd(263, 3) = 1 \quad \checkmark$$
$$3^{131} \equiv 1 \mod 263 \quad \checkmark$$

$$\gcd(263, 5) = 1 \quad \checkmark$$
$$5^{131} \equiv -1 \mod 263 \quad \checkmark$$

Therefore 263 is prime with probability $1 - 4^{-3} = 0.984375$.

Question 3

Factor $n = 110545695839248001$ using the Pollard rho method with $a_0 = 1$ and $c = 1$.

Solution:

We use the following code to get the factorization of n. We first implement n as is. After that we run the same script for n devided by the found factors. Until n itself is prime. We use $a_0 = b_0 = 1$ and start the script from $i = 1$ because $a_0 - b_0 = 0$.

3/3

```
n = 110 545 695 839 248 001;
a = 2;
b = 5;
c = 1;
While[GCD[a - b, n] = 1,
 a = Mod[a^2 + c, n];
 b = Mod[(b^2 + c)^2 + c, n];
]
GCD[a - b, n]
```

We find that n can be factorized into $479909 \cdot 479939 \cdot 479951$.

Question 4

Factor $n = 530989802569251535920 47$ using the $p - 1$ method with $B = 128$ and $a = 2$.

Solution:

We use the following code to get the factorization of n. We first implement n as is. After that we run the same script for n devided by the found factors. Until n itself is prime.

1/3

```
n = 53 098 980 256 925 153 592 047;
a = 2;
B = 128;
m = 1;
While[Prime[m] < B,
  k = 1;
  While[Prime[m] ^ k < B, k++];
  a = Mod[a ^ (Prime[m] ^ (k - 1)), n];
  m ++;
 ];
GCD[a - 1, n]
m = 32;
new = a - 1;
While[GCD[new, n] == 1,
  new = Mod[new * (a ^ Prime[m] - 1), n];
  m ++;
 ];
GCD[new, n]
```

With this program we found that we can factorize n into $479971 \cdot 480043 \cdot 480059 \cdot 480061$

you did not find all these factors without changing B