Technical University of Denmark

01410 Cryptology 1

Homework 3

Authors:

Andreas Hallberg Kjeldsen
s092638@student.dtu.dk

Morten Chabert Eskesen
s133304@student.dtu.dk

May 5, 2014

Exercise 3.1

3.1.1

We have to show that $n + d^2$ is a square in $\mathbb{Z}$ where $q - p = 2d > 0$ and $n = pq$ and d, p and q are integers.

$$n + d^2 = pq + (\tfrac{q-p}{2})^2 = pq + \tfrac{q^2}{4} + \tfrac{p^2}{4} - \tfrac{pq}{2} = \tfrac{q^2}{4} + \tfrac{p^2}{4} + \tfrac{pq}{2} = (\tfrac{p+q}{2})^2$$

Now $p + q = 2d + 2p$ so $\frac{p+q}{2} \in \mathbb{Z}$. This show that $n + d^2$ is a square in $\mathbb{Z}$.

3.1.2

Given two integers n and d where n is the product of two odd primes p and q and d is a small integer defined as in 3.1.1. We have to show how this information can be used to factor n. The primes p and q must be close to each other since $d > 0$ is a small integer given as $\frac{q-p}{2}$ and $q > p$. Since

$$n = (\frac{q+p}{2})^2 - d^2$$

We define the integer u as $u = \frac{p+q}{2}$. u can only be slightly larger than $\sqrt{n}$ and $u^2 - n$ is a square in $\mathbb{Z}$. Therefore we can try the following:

$$u = \lceil \sqrt{n}\ \rceil + k, \quad k = 0, 1, 2, \ldots$$

We try this until u becomes a square in $\mathbb{Z}$. Then we calculate the two primes p and q by $p = u - d$ and $q = u + d$ since $n = pq$ with $q > p$ and $n = (\frac{q+p}{2})^2 - d^2$.

3.1.3

We will use the technique from 3.1.2 to factor $n = 551545081$. We find $\sqrt{n} \approx 23484.99\ldots$. We therefore begin our technique with $k = 0$ and find that $u = 23485$.

$$d = \sqrt{u^2 - n} = \sqrt{23485^2 - 551545081} = 12$$

We then get that:
$p = u - d = 23485 - 12 = 23473$ and
$q = u + d = 23485 + 12 = 23497$

Exercise 3.2

3.2.1

Let n be a product of two odd, distinct primes p_1 and p_2. We have to find the maxmium order of an element modulo n.

Let r_1 be a primitive root mod p_1 and let r_2 be a primitive root mod p_2 and let $t = \text{lcm}(p_1 - 1, p_2 - 1)$. We use the Chinese Remainder Theorem to find an x such that:

$$x \equiv r_1 \bmod p_1$$
$$x \equiv r_2 \bmod p_2$$

We have to show the following:

1. $x^t \equiv 1 \bmod p_1p_2$.
2. If $0 < k < t$, then $x^k \not\equiv 1 \bmod p_1p_2$.
3. If y $\in (\mathbb{Z}_{p_1p_2}\mathbb{Z})^*$, then $y^t \equiv 1 \bmod p_1p_2$.

3.2.2

Let $n = 2051152801041163$ (product of two primes) and define the hash function

$$H_F(m) = 8^m \bmod n$$

for $m \in \mathbb{Z}$. The order of 8 modulo n is the maximum possible.
Let $p = 2189284635404723$ which is a prime and $\frac{p-1}{2}$ is also a prime.
We have to find a primitive element $\alpha \in \mathbb{Z}_p^*$ and choose a valid, private key $a \in \mathbb{Z}_{p-1}$. The only prime factors in $|\mathbb{Z}_p^*| = p - 1$ are 2 and $\frac{p-1}{2}$ since $\frac{p-1}{2}$ is prime. The order of an element must divide $p - 1$ therefore there are only 4 possible orders: 1 (the identity), 2 (the element - 1), $\frac{p-1}{2}$ and $p - 1$ (the primitive elements).
Any element $\alpha \not\equiv \pm 1 \bmod p$ such that $\alpha^{\frac{p-1}{2}} \not\equiv 1 \bmod p$ must have the order $p - 1$ and therefore it is primitive.
We use $\alpha = 42$ and use the following command in Maple.

```
p:=2189284635404723: 42&^((p-1)/2) mod p;
```

This shows us that $42^{\frac{p-1}{2}} \not\equiv 1 \bmod p$. It is also clear that $42^2 \not\equiv 1 \bmod p$. Therefore 42 has order $p - 1$ and it is primitive in $\mathbb{Z}_p^*$.
We choose the private key $a \in \mathbb{Z}_{p-1}$ at random. Which gives us $a = 815782344718261$.

3.2.3

We have to use α, a and p to set up the El-Gamal digital signature system. m is an integer describing a 6-digit DTU student number where the leading 0 is discarded if there is any. We compute the signature of m using the El-Gamal system with the hash function H_F and the "random" number $k = 1234567$.
We use Morten's student number (133304) as the message, $m = 133304$. We hash m with H_F and we get the following:

$$H_F(133304) \equiv 8^{133304}$$
$$H_F(133304) \equiv 1327930088214640 \bmod 2051152801041163$$

Now we have our value of x. The signature $(\gamma,\, \delta) \in \mathbb{Z}_p \times \mathbb{Z}_{p-1}$ is then given as:

$$\gamma \equiv 42^{1234567}$$
$$\gamma \equiv 2076571105570857 \bmod 2189284635404723$$
$$\delta \equiv (1327930088214640 - 815782344718261 * 2076571105570857)(1234567)^{-1}$$
$$\delta \equiv -1694030045476783892477149105037 * 427810349476471$$
$$\delta \equiv 1297737808822113 \bmod 2189284635404722$$

Therefore $(\gamma,\, \delta) = (2076571105570857,\, 1297737808822113)$. We found the multiplicative inverse of 1234567 in $\mathbb{Z}^*_{p-1}$ by using the following command in Maple:

```
1234567^(-1) mod 2189284635404722
```

One could also use Euclid's extended algorithm.

3.2.4

We have to show that the signature produced in 3.2.3 will be verified as the signature on m. In order to check that $(\gamma,\, \delta) = (2076571105570857,\, 1297737808822113)$ is verified as the signature on m the following must hold.

$$(\alpha^a)^\gamma \gamma^\delta \equiv \alpha^x \bmod p$$

We start by computing the left-hand side individually.

$$(\alpha^a)^\gamma \equiv (42^{815782344718261})^{2076571105570857} \equiv 1330881686950231 \bmod 2189284635404723$$
$$\gamma^\delta \equiv 2076571105570857^{1297737808822113} \equiv 1584897462290462 \bmod 2189284635404723$$

$(\alpha^a)^\gamma \gamma^\delta \equiv 571999655777925 \bmod 2189284635404723$
The right-hand side is

$$\alpha^x \equiv 42^{1327930088214640} \equiv 571999655777925 \bmod 2189284635404723$$

Therefore $(\alpha^a)^\gamma \gamma^\delta \equiv \alpha^x \bmod p$ is fulfilled, thus showing that $(\gamma,\, \delta) = (2076571105570857,\, 1297737808822113)$ is verified as the signature on m.