Cryptography I
Exercise sheet 5

Ilja Kuzovkin

October 20, 2010

1 Exercise 5a

We have composite number n and we know that for one of it's factors p $p-1$ is powersmooth number. For solving that problem we can use Pollard's p-1 algorithm[1], implementation of which you will find in file *exercise5a.py*.

n factors are

```
p1 = 86194768618716286465819334092683429114930567699119082576117223017384723012
     75434959902175061220850111320122444300974234054494495326036638077800290674
     37019
p2 = 23917629537681961393203914587699227771929908038649708207338757455681390410
     37286153954600967544623389052416123539590853837707285234726557342262967388
     199
```

2 Exercise 5b

We know

$$c_1 = m^2 \ mod \ n$$
$$c_2 = (am+b)^2 \ mod \ n$$

where c_1, c_2, n, a, b are known and we want to find m.
From two equations above we can build an equation which will give us m:

$$c_2 = (am+b)^2 \ mod \ n$$
$$c_2 = a^2m^2 + 2abm + b^2 \ mod \ n$$

we can replace m^2 by c_1, which will give us

$$c_2 = a^2c_1 + 2abm + b^2 \ mod \ n$$
$$2abm = c_2 - a^2c_1 - b^2 \ mod \ n$$
$$m = (c_2 - a^2c_1 - b^2) * (2ab)^{-1} \ mod \ n$$

The calculation is performed in the *execrise5b.py* file. Also checks are performed there, to make sure message we got is the right one.
Answer is:

```
m = 28798088478899060656702144501781850487589091276111705937701204382607585876 2
    39580384740911083951862738428821782433942449849488357597029098995216334424 03
```

References

[1] http://en.wikipedia.org/wiki/Pollard's_p_-_1_algorithm