AARHUS UNIVERSITET, SCIENCE, COMPUTER SCIENCE

Cryptography - Handin 6

Peter Burgaard - 201209175

October 13, 2016

1 STINSON 5.10

Prove that:

$$x \in \mathbb{Z}_n^* \implies d(e(x)) = x$$

We know that $e(x) = x^b \mod n$, and $d(y) = y^a \mod n$, from the exercise description. We know from Stinson, chapter 5, $n = pq$, where p and q are primes where $p \neq q$, and that $ab \equiv 1 \mod (p-1)(q-1)$. The exercise also mentions as a hint that $x_1 \equiv x_2 \mod p \cdot q \iff x_1 \equiv x_2 \mod p$ and $x_1 \equiv x_2 \mod q$ which follows from Stonson, Theorem 5.3.

Our goal is to show

$$d(y) = d(e(x)) \equiv \left(x^b\right)^a \equiv x \mod n$$

Proof.

We will approach this by dividing x into an expression with an 'inner' exponent and an 'outer' exponent. Lets make p the 'inner'. By Stinson 5.3

$$\left(x^b\right)^a \equiv x^{t\phi(n)+1} \mod n \equiv x^{t(p-1)(q-1)+1} \equiv x \cdot \left(x^{(p-1)}\right)^{t(q-1)}$$

for some integer $t \geq 1$. Its obvious that if $p * q | x \implies p | x$. So, since p is assumed to be a prime, we can derive from Fermat little theorem[1]:

$$x \cdot \left(x^{(p-1)}\right)^{t(q-1)} \equiv x \cdot 1^{t(q-1)} \mod p \implies \left(x^b\right)^a \equiv x \mod p$$

[1] Suppose p is a prime and $a \in \mathbb{Z}$ where $p \nmid a$, then $a^{p-1} \equiv 1 \mod p$

The same proof can be done for p as a divider, and by the clue in the exercise we get

$$\left(x^b\right)^a \equiv x \mod p \cdot q \iff \begin{cases} \left(x^b\right)^a \equiv x \mod p \\ \left(x^b\right)^a \equiv x \mod q \end{cases}$$

And since $p \cdot q = n$, then we are done. $\square$

2 STINSON 5.10 - CONTINUED

Prove:

$$x \in \mathbb{Z}_n \implies d(e(x)) = x$$

Proof.

Since we made no assumptions about $x \in \mathbb{Z}_n^*$, the proof above must also hold for $x \in \mathbb{Z}_n$ $\square$