Dr. Michael Reyer

Tutorial 1

Friday, October 26, 2018

Problem 1. *(Rabin cryptosystem)* Alice and Bob are using the Rabin Cryptosystem. Bob uses the public key $n = 4757 = 67 \cdot 71$. All integers in the set $\{1, \dots, n-1\}$ are represented as a bit sequence of 13 bits. In order to be able to identify the correct message, Alice and Bob agreed to only send messages with the last 2 bits set to 1. Alice sends the cryptogram $c = 1935$. Decipher this cryptogram.

Problem 2. *(coin flipping)* Let p be prime and $p \equiv 3 \pmod 4$.

a) Show that if $x \equiv -x \pmod p$, then $x \equiv 0 \pmod p$.

b) Suppose $x, y \not\equiv 0 \pmod p$ and $x^2 \equiv y^2 \pmod{p^2}$. Show that $x \equiv \pm y \pmod{p^2}$.
Hint: Prop 6.8 might be of help.

c) Let c be a QR $\mod p^2$, $b = c^{\frac{p+1}{4}} \mod p$, $a = \frac{c-b^2}{p} 2^{-1} b^{-1} \mod p$ and $x = b + ap$. Then $x^2 \equiv c \pmod{p^2}$. Calculate x for $p = 7$ and $c = 37$.

Consider the coin flipping protocol. Alice cheats by choosing $n = pq = p^2$.

d) Suppose that Bob suspects that Alice has cheated. Can Bob discover her attempt to cheat? Can Bob use the cheating as an advantage for himself?

e) Show that Bob almost always loses if he trusts Alice. In which cases should Bob get suspicious?