T-79.5501 Cryptology
Second midterm exam
May 7th, 2007
Each problem is worth 6 points.
Suomenkielinen koe toisella puolella.

1. Let $n = 323 = 17 * 19$. Solve

$$x^2 - 10x + 24 \equiv 0 \pmod{n}.$$

2. Consider a finite field $\mathbb{F} = \mathbb{Z}_2[x]/(x^3+x+1)$. Let an S-box with three input bits and three output bits be defined using the function $\pi_S(w) = w^3$, for $w \in \mathbb{F}$. For example, if $w = \texttt{011} = x+1$ then $\pi_S(w) = \pi_S(x+1) = (x+1)^3 = x^3+x^2+x+1 = x^2 = \texttt{100}$.

   a) (3 points) Let $a' = \texttt{100} = x^2$. Show that

$$\pi_S(w + a') + \pi_S(w) = x^2w^2 + (x^2 + x)w + x^2 + 1, \text{ for all } w \in \mathbb{F}.$$

   b) (3 points) Compute the row of the *Difference Distribution Table* of $\pi_S$ corresponding to the input difference $a' = \texttt{100}$. Note that you can use the result of item a).

3. Your RSA modulus is $1055 = 5 * 211$, and you select your public exponent to be $b = 11$. Compute your private key and decrypt the ciphertext $y = 314$.

4. Element $\alpha = 202$ is of order 16 in the multiplicative group $\mathbb{Z}^*_{2005}$. It is given that element $\beta = 133$ is in the subgroup generated by $\alpha$. Using Shank's algorithm compute the discrete logarithm $x$ of $\beta = 133$ to the base $\alpha = 202$, that is, solve the equation

$$202^x \equiv 133 \,(\mathrm{mod}\, 2005).$$

T-79.5501 Foundations of Cryptology
Toinen välikoe
7.5.2007
Jokaisesta tehtävästä saa 6 pistettä.
English text on the other side.

1. Olkoon $n = 323 = 17 * 19$. Ratkaise

$$x^2 - 10x + 24 \equiv 0 \pmod{n}.$$

2. Tutkitaan äärellistä kuntaa $\mathbb{F} = \mathbb{Z}_2[x]/(x^3 + x + 1)$. Olkoon annettuna S-laatikko (S-box), jolla on kolme syötebittiä (input bits), kolme tulostebittiä (output bits) ja S on määritelty käyttämällä funktiota $\pi_S(w) = w^3$, missä $w \in \mathbb{F}$. Esimerkiksi, jos $w = \mathtt{011} = x + 1$, niin $\pi_S(w) = \pi_S(x + 1) = (x + 1)^3 = x^3 + x^2 + x + 1 = x^2 = \mathtt{100}$.

   a) (3 pist.) Olkoon $a' = \mathtt{100} = x^2$. Näytä, että

$$\pi_S(w + a') + \pi_S(w) = x^2w^2 + (x^2 + x)w + x^2 + 1, \text{ kaikille } w \in \mathbb{F}.$$

   b) (3 pist.) Laske $\pi_S$:n *Differenssijakaumataulukon* (Difference distribution table) se rivi, jossa syötedifferenssi on $a' = \mathtt{100}$. Huomaa, että voit käyttää a-kohdan tulosta.

3. RSA-moduli on $1055 = 5 * 211$, ja julkinen eksponentti on $b = 11$. Laske salainen avain ja tulkitse salakieli $y = 314$.

4. Alkion $\alpha = 202$ kertaluku on 16 multiplikatiivisessa ryhmässä $\mathbb{Z}^*_{2005}$. Tiedetään että alkio $\beta = 133$ on alkion $\alpha$ generoimassa aliryhmässä. Määritä Shanksin menetelmällä alkion $\beta = 133$ diskreetti logaritmi $x$ kannan $\alpha = 202$ suhteen, eli ratkaise yhtälö

$$202^x \equiv 133 \,(\mathrm{mod}\, 2005).$$