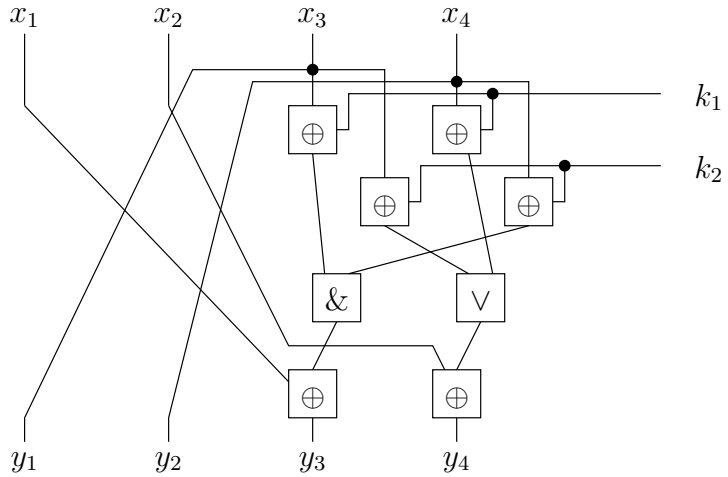
Krüptoloogia I eksam

4. november 2008

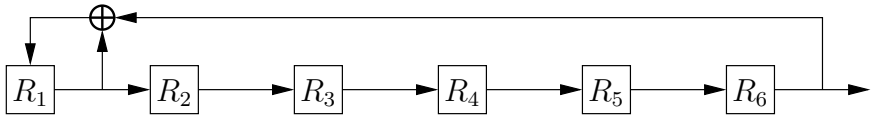
1. Viskame kaks korda tasakaalustatud 6-tahulist täringut. Olgu $\mathbf{Z}_1$ ja $\mathbf{Z}_2$ juhuslikud muutujad, mille väärtuseks on vastavalt esimese ja teise viske tulemus. Olgu $\mathbf{X} = \mathbf{Z}_1 + \mathbf{Z}_2$ ja $\mathbf{Y} = \mathbf{X} \bmod 4$. Leia $H(\mathbf{X}|\mathbf{Y})$.

2. Vaatleme järgmist „iteratiivselt konstrueeritud plokkšifri raundifunktsiooni“ (tegelikult peavad plokid pikemad olema) $y = F(x, k)$:



   Leia üheraundilise karakteristiku $0110 \xrightarrow{p} 1000$ tõenäosus p.

3. Vaatame järgmist LFSR-i. Olgu alguses kõigi registrite sisuks bitt 1.



   Kas leidub lühemaid LFSR-e, mis genereerivad sama võtmejada?

4. Näita, et sümmeetrilise krüptosüsteemi konstrueerimisel plokkšifrist CTR-moodi kasutades ei saa me süsteemi, mis oleks turvaline valitud krüptotekstiga rünnete vastu.

5. Olgu E mingi plokkšifri krüptimisfunktsioon, kus nii ploki kui ka võtme pikkus on n. Defineerime kompressioonifunktsiooni $H(x, y) = E_x(y) \oplus E_y(x) \oplus y$. Defineerime ka räsifunktsiooni $H^* : (\{0,1\}^n)^* \to \{0,1\}^n$ valemiga

$$H^*(x_1 \cdots x_m) = H(H(\cdots H(H(Z, x_1), x_2) \cdots), x_{m-1}), x_m),$$

   kus Z on n-st nullbitist koosnev jada. Näita, et H^* pole kollisioonikindel.
   Vihje. Uuri avaldist $H(x, x)$.

6. Vaatame järgmist kinnistusskeemi. Olgu G rühm, kus Diffie-Hellmani otsustusprobleem on raske. Olgu $|G| = p$, kus p on algarv. Olgu g selle rühma moodustaja. Olgu $h \in G$, nii et mitte keegi ei tea suurust $\log_g h$ (elemendid g ja h ise on avalikud). Selleks, et kinnistada suurust $x \in \mathbb{Z}_p$, genereeri juhuslikult $r \in \mathbb{Z}_p$ ja arvuta välja kinnistus $c = g^x h^r$. Kinnistuse avamiseks saada x ja r. Näita, et see kinnistusskeem on turvaline.

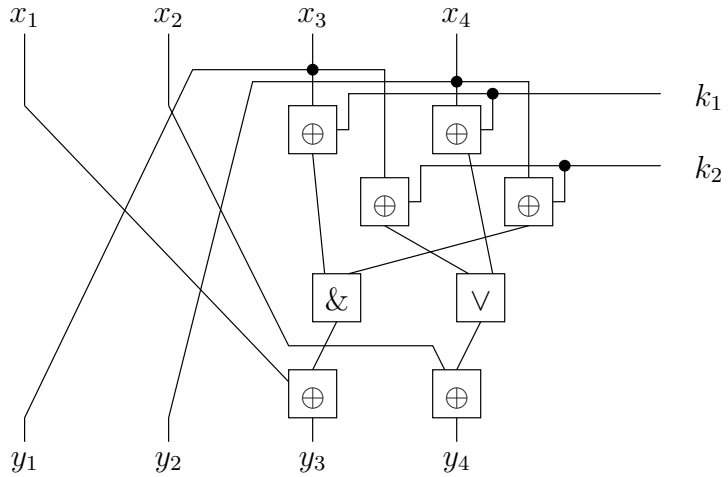
Eksam moodustab ühe kolmandiku koguhindest.
Kõik eksamiülesanded on võrdse kaaluga.

Exam in Cryptology I

November 4th, 2008

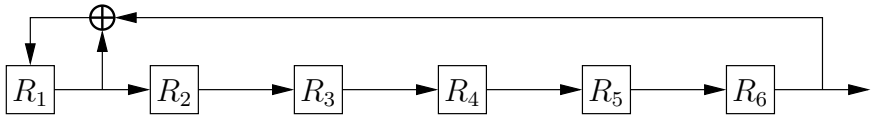
1. Let us throw a fair six-sided die twice. Let $\mathbf{Z}_1$ and $\mathbf{Z}_2$ be the random variables equal to the results of the first and second throw. Let $\mathbf{X} = \mathbf{Z}_1 + \mathbf{Z}_2$ and $\mathbf{Y} = \mathbf{X} \bmod 4$. Find $H(\mathbf{X}|\mathbf{Y})$.

2. Consider the following "round function of an iteratively constructed block cipher" (too short blocks for real life) $y = F(x, k)$:



   Find the probability p of the one-round characteristic $0110 \xrightarrow{p} 1000$.

3. Consider the following LFSR. Let all registers initially contain the bit 1.



   Are there any shorter LFSR-s that generate the same keystream?

4. Show that the construction of a symmetric encryption system from a block cipher using the CTR mode of operation will not give us a system that is secure against chosen-ciphertext attacks.

5. Let E be the encryption function of some block cipher whose key length and block length are both equal to n. Define the compression function $H(x, y) = E_x(y) \oplus E_y(x) \oplus y$. Also define the hash function $H^* : (\{0,1\}^n)^* \to \{0,1\}^n$ by

$$H^*(x_1 \cdots x_m) = H(H(\cdots H(H(Z, x_1), x_2) \cdots), x_{m-1}), x_m)$$

   where Z is the bit-string of n zeroes. Show that H^* is not collision-resistant.
   Hint. Consider $H(x, x)$.

6. Consider the following commitment scheme. Let G be a group with a hard decisional Diffie-Hellman problem and g be a generator of that group. Let $|G| = p$, where p is prime. Let $h \in G$, such that noone knows $\log_g h$ (both g and h are public). To commit to a number $x \in \mathbb{Z}_p$, generate a random $r \in \mathbb{Z}_p$ and compute the commitment $c = g^x h^r$. To open the commitment, send x and r. Show that this scheme is secure.

The exam makes up one third of the final grade.
All exercises in the exam have equal weight.