Krüptoloogia I eksam

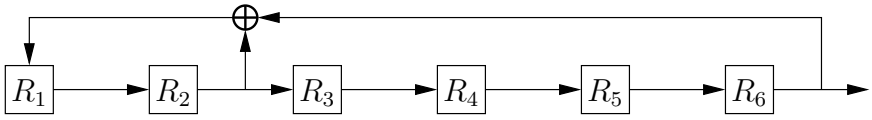
6. jaanuar 2009

1. Vaatame funktsiooni $F(x,k) = S(x_1, x_2, x_3 \oplus k_1, x_4 \oplus k_2)$, kus $x \in \{0,1\}^4$, $k \in \{0,1\}^2$ ja S on defineeritud järgmiselt:

z	$S(z)$	z	$S(z)$	z	$S(z)$	z	$S(z)$
0000	1101	0100	1111	1000	0011	1100	0101
0001	0010	0101	0100	1001	0111	1101	1010
0010	1011	0110	1001	1010	1000	1110	0000
0011	1110	0111	0110	1011	1100	1111	0001

   Leia F-i üheraundilise karakteristiku $0110 \xrightarrow{p} 1000$ tõenäosus p. S.t. kui juhuslikult valida x, x^*, k, nii et $x \oplus x^* = 0110$, siis mis on tõenäosus, et $F(x,k) \oplus F(x^*,k) = 1000$?

2. Vaatame järgmist LFSR-i. Olgu alguses kõigi registrite R_1 ja R_3 sisuks bitt 0 ja ülejäänute sisuks bitt 1.



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

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

4. Olgu $E = \{E_i\}_{i \in I}$ ja $F = \{F_i\}_{i \in I}$ kaks ühesuunaliste funktsioonide peret. Defineerime $G_i(x) = E_i(x) \cdot F_i(x)$ (loeme, et E_i-l ja F_i-l on sama muutumispiirkond ning sellel on defineeritud korrutamine). Too näide sellistest ühesuunaliste funktsioonide peredest (oletades mingite standardsete krüptograafiliste keerukus) E ja F, nii et pere $\{G_i\}_{i \in I}$ ei oleks ühesuunaline.

5. Alice ja Bob kavatsevad kasutada ElGamali signatuuriskeemi, Alice signeerijana ja Bob verifitseerijana. Nad on kokku leppinud algarvu p, nii et $\mathbb{Z}_p^*$ on skeemis kasutatav rühm. Alice genereerib rühma $\mathbb{Z}_p^*$ mingi moodustaja g, oma salajase võtme $\alpha \in \mathbb{Z}_{p-1}$ ja arvutab avaliku võtme $\chi = g^\alpha$. Ta saadab g ja χ (autentsel viisil) Bobile. Bob salvestab need suurused.

   Kahjuks selgub, et koht, kuhu Bob salvestas suuruse g, on ründaja poolt muudetav. Kuidas saab ründaja Bobi jaoks võltsida Alice'i signatuure suvalistele teadetele?

6. Mis on nullteadmustõestused? Kuidas on defineeritud nullteadmus ja miks see oluline on?

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

Exam in Cryptology I

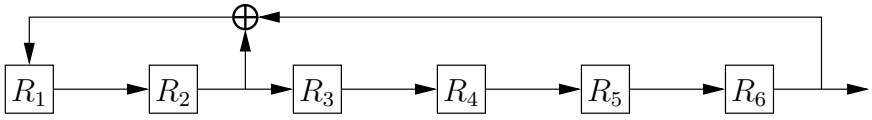
January 6th, 2009

1. Consider the function $F(x,k) = S(x_1, x_2, x_3 \oplus k_1, x_4 \oplus k_2)$, where $x \in \{0,1\}^4$, $k \in \{0,1\}^2$ and S is defined as follows:

z	$S(z)$	z	$S(z)$	z	$S(z)$	z	$S(z)$
0000	1101	0100	1111	1000	0011	1100	0101
0001	0010	0101	0100	1001	0111	1101	1010
0010	1011	0110	1001	1010	1000	1110	0000
0011	1110	0111	0110	1011	1100	1111	0001

   Find the probability p of the one-round characteristic $0110 \xrightarrow{p} 1000$ of F. I.e. if x, x^*, k are chosen randomly, such that $x \oplus x^* = 0110$ then what is the probability of $F(x,k) \oplus F(x^*,k) = 1000$?

2. Consider the following LFSR. Let the initial contents of R_1 and R_3 be 0 and the contents of other registers be 1.



   Do there exist shorter LFSR-s generating the same keystream?

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

4. Let $E = \{E_i\}_{i \in I}$ and $F = \{F_i\}_{i \in I}$ be two families of one-way functions. Define $G_i(x) = E_i(x) \cdot F_i(x)$ (we assume that E_i and F_i have the same range, and a multiplication operation has been defined over it). Give an example of such one-way function families (under standard cryptographic assumptions) E and F, such that $\{G_i\}_{i \in I}$ is not one-way.

5. Alice (signer) and Bob (verifier) intend to use the ElGamal signature scheme. They have agreed on a prime number p, such that $\mathbb{Z}_p^*$ is the group used by the scheme. Alice generates some generator g of $\mathbb{Z}_p^*$, her secret key $\alpha \in \mathbb{Z}_{p-1}$, and computes her public key $\chi = g^\alpha$. She sends g and χ to Bob (over some authentic channel). Bob stores those quantities.

   Unfortunately, it turns out that the memory where Bob has stored g can be tampered by the adversary. How can the adversary forge Alice's signatures for Bob, and for arbitrary messages?

6. What are zero-knowledge proofs? How is zero-knowledge defined and why is it important?

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