Krüptoloogia I eksam

29. jaanuar 2007

1. Kuidas käib kolmeraundilise DES-i diferentsiaalne krüptoanalüüs?

2. Kuidas töötab ElGamali krüptosüsteem? Millise (arvuteoreetilise) probleemi arvatav raskus on samaväärne ElGamali süsteemi turvalisusega? Sõnasta ka see probleem ja anna ekvivalentsuse-tõestus.

3. Mis on signatuuriskeemide juures eksistentsiaalne võltsing (*existential forgery*)? Miks neid vältima peaks? Kuidas täiendada signatuuriskeeme nii, et eksistentsiaalsed võltsimised rasked oleksid?

4. Mis on räsifunktsioon ja milleks seda kasutatakse? Millal on räsifunktsioon kindel originaali leidmise suhtes / kindel teise originaali leidmise suhtes / kollisioonikindel? Kuidas käib signeerimine koos räsimisega ja millist omadust räsifunktsiooni siis rahuldama peab ja miks?

5. TEA (*Tiny Encryption Algorithm*) on blokkšiffer, mille blokipikkus on 64 bitti ja võtmepikkus 128 bitti. TEA-l on ekvivalentseid võtmeid: Kui $K \in \{0,1\}^{128}$ ning K' on saadud K-st tema 1. ja 33. biti väärtust muutes (0-st 1-ks või vastupidi), siis $\mathrm{TEA}_K(\cdot) = \mathrm{TEA}_{K'}(\cdot)$. Samuti, kui K'' on saadud K-st tema 65. ja 97. biti väärtust muutes, siis $\mathrm{TEA}_K(\cdot) = \mathrm{TEA}_{K''}(\cdot)$. Veel ühe K-ga ekvivalentse võtme saame, kui muudame ära kõigi nelja mainitud biti väärtuse.

   Defineerime kompressioonifunktsiooni $H(x_1, x_2) = \mathrm{TEA}_{x_1}(\mathrm{msb}_{64}(x_1) \oplus x_2) \oplus \mathrm{lsb}_{64}(x_1) \oplus x_2$, kus $x_1 \in \{0,1\}^{64}$ ja $x_2 \in \{0,1\}^{128}$. Tehtemärkidest tähendab $\oplus$ bitikaupa välistavat võid ning $\mathrm{msb}_k(x)$ [vastavalt: $\mathrm{lsb}_k(x)$] võtab k vasakpoolsemat [vastavalt: parempoolsemat] bitti bitijadast x.

   Ülesanne: leida H-ile kollisioon.

6. Näita, et blokkšifri kasutamine CBC-moodis ei anna meile veel krüptosüsteemi, mis oleks turvaline valitud krüptotekstiga rünnete vastu. S.t. konstrueeri vastane $\mathcal{A}$, mis ründab saadud krüptosüsteemi (millise definitsiooni mõttes, võid ise valida), kasutab vähe ressursse, kuid on suure eelisega, isegi kui blokkšiffer on pseudojuhuslik funktsioon.

Iga ülesanne annab kuni 5 punkti. Materjale tohib kasutada.
Iga lahendatud koduse ülesande eest saab 10 punkti.