Krüptoloogia I eksam

6. november 2007

1. Vaatleme ElGamal-i signatuuriskeemi mingis tsüklilises rühmas G (kus diskreetse logaritmi ülesanne on raske), olgu $m = |G|$ ja olgu g rühma G moodustaja. Olgu meil teada verifitseerimisvõti χ, kuid mitte signeerimisvõti α. Samuti olgu meil teada, et skeemi vaadeldav implementatsioon on selline, kus signeerimisel kasutatavate juhuarvude genereerimiseks kasutatakse lineaarset kongruentsiaalset generaatorit, s.t. kui mingil signeerimisel kasutati juhuarvu r, siis järgmisel kasutatakse juhuarvu $(ar + b) \bmod m$ mingite fikseeritud ja meile teada arvude $a \in \mathbb{Z}_m^*, b \in \mathbb{Z}_m$ jaoks.

   Kirjelda, kuidas signeerimisvõtit α teadmata signeerida ükskõik millist teadet m. See signatuuri võltsimise protseduur tohib välja kutsuda meetodit *juhuslik_signatuur*, mis tagastab mingi juhusliku teate m' ja sellele vastava signatuuri.

2. Olgu h_1 ja h_2 kaks räsifunktsiooni ning olgu $h(x) = h_1(h_2(x))$. Näita, et kui h_2 on kindel teise originaali leidmise suhtes, kuid h_1 ei ole, siis h võib nii olla kui ka mitte olla kindel teise originaali leidmise suhtes. S.t. too näited funktsioonidest h_1 ja h_2 mõlema juhu jaoks.

3. Olgu $\mathbf{X}$ ühtlaselt jaotunud juhuslik muutuja üle n-elemendilise hulga X. Olgu $\kappa : X \to \{0,1\}^*$ hulga X mingi prefiksivaba kodeering, nii et $\kappa(\mathbf{X})$ keskmine pikkus on nii väike kui võimalik. Millega võrdub see keskmine pikkus? Kui palju erineb ta $\mathbf{X}$-i entroopiast?

4. Mis on nullteadmustõestused?

5. Kuidas käib kolmeraundilise DES-i diferentsiaalne krüptoanalüüs?

6. Olgu (n, e_1) ja (n, e_2) kahe osapoole avalikeks võtmeteks RSA krüptosüsteemis. Kuidas saab üks neist osapooltest murda krüptotekste, mis on krüptitud teise osapoole avaliku võtmega?

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

Exam in Cryptology I

November 6th, 2007

1. Consider the ElGamal signature scheme in some cyclic group G (where the discrete logarithm problem is hard). Let $m = |G|$ and let g be a generator of G. Let the verification key χ be known to us, but the signing key α be unknown. We also know that in the implementation of the signing functionality, the linear congruential generator has been used to generate the random numbers. I.e. if the random number r was used to generate a signature, then $(ar + b) \bmod m$ will be used as the randomness in the next signature. Let a and b be known to us.

   Describe how we can forge a signature for any message m of our choice. The forging algorithm is allowed to invoke the method *random_sig* that returns a randomly chosen message m' and the signature corresponding to it.

2. Let h_1 and h_2 be two hash functions and let $h = h_1(h_2(x))$. Show that if h_2 is second preimage resistant, but h_1 is not, then h may or may not be second preimage resistant. I.e. give examples of the functions h_1 and h_2 for both cases.

3. Let $\mathbf{X}$ be a uniformly distributed random variable over the set X of cardinality n. Let $\kappa : X \to \{0,1\}^*$ be a prefix-free encoding of the set X, such that the average length of $\kappa(\mathbf{X})$ is as small as possible. What is the value of this average length? How much does it differ from the entropy of $\mathbf{X}$?

4. What are zero-knowledge proofs?

5. Describe the differential cryptanalysis of three-round DES.

6. Let (n, e_1) and (n, e_2) be the public keys of two parties in the RSA encryption system. How can one of those parties break the cryptotexts that have been encrypted with the other party's public key?

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