T-79.4501 Tiedon salaus ja suojaus
Tentti 6.3.2006

1. (6 pist) Salakieliteksti

AYXHK XRGZE RIRCL ONESU RCKFE KRFXS MNSMK MSCMS KVTNE NNIWN SHGWN KZEXP
ELXHO WOCRD USRYX EVWOG ONUAL KHGKS FUREU XHKVC APTAV EYLOA PDYLA XTETS
UXEBO PIZCT UWCXY TORIF IMUVE YXEGH IRCTU EPVVE IMAZI MUVER SVORG RCOAV
OCR

on luotu *Vigenerin siirtomenetelmällä.* Arvioi Kasiskin menetelmällä avaimen pituutta (jaksoa).

2. (a) (3 pist) Mitä on kolminkertainen salaus? Mitä etua siitä on kaksinkertaiseen salaukseen verrattuna?

   (b) (3 pist) Miksi keskimmäinen operaatio 3DES salausoperaatiossa ei ole salaus vaan tulkinta?

3. (6 pist) Esitä *Polynomial MAC* viestin autentikointimenetelmän toimintaperiaate.

4. (6 pist) Alice käyttää DSA allekirjoitusmenetelmän pientä leikkiversiota, jossa alkulukumoduuli on $p = 43$ ja generaattori on $g = 21$ kertalukua $q = 7$. Alice allekirjoittaa vahingossa kaksi viestiä samalla viestikohtaisella satunnaisluvulla $k$. Allekirjoitettujen viestien hash-koodit ovat 2 ja 3, ja allekirjoitukset ovat (2, 1) ja (2, 6), vastaavasti. Määritä Alicen salainen avain.

5. (6 pist) Tarkastellaan kahta lukugeneraattoria mustina laatikkoina, jolloin näemme vain niiden tuottamat lukujonot. Kumpikin generaattori tuottaa 64-bittisiä lukuja. Lisksi tiedetään, että toinen mustista laatikoista sisältää laskurimoodigeneraattorin (Counter Mode PRNG), joka käyttää IDEA salausoperaatiota funktiona $E_K$ ja laskuria, jonka pituus on 64 bittiä. Toinen musta laatikko sisältää todellisen satunnaislukugeneraattorin. Päältäpäin laatikot näyttävät aivan samalta ja tehtävänä on pelkästään tuotettuja jonoja tutkimalla määrätä kumpi laatikoista on todellinen satunnaislukugeneraattori. Kun molemmat generaattorit ovat tuottaneet noin $2^{32}$ lukua, mahdollisuudet ovat vähintään 50% että pystytään sanomaan kumpi on kumpi. Kuinka se on mahdollista?

Muista täyttää kurssipalaute. Linkki on kurssin kotisivulla.

tehtä. 4.

$r = (g^k \bmod p) \bmod q$

$s = k^{-1}(H + r \cdot x) \bmod q$