T-79.4501 Tiedon salaus ja suojaus
TENTTI
3.9.2008

1. (6 pist) *Atbash cipher* on yksinkertainen korvausmenetelmä, joka vain kääntää aakkoston, eli salaa kirjaimen A kirjaimeksi Z, kirjaimen B kirjaimeksi Y, kirjaimen C kirjaimeksi X, jne. Englannin kielen aakkosilla. Tarkastellaan kaksinkertaista salausta *Atbash cipher*- ja *Shift cipher*-menetelmiä käyttäen Englannin kielen aakkosilla. Yleensä nämä menetelmät eivät ole vaihdannaiset keskenään, mikä tarkoittaa sitä että kun ensin salataan *Atbash*-menetelmällä ja sen jälkeen *Shift*-menetelmällä, niin tulos on eri kuin jos salataan *Shift*-menetelmällä ensin ja sitten *Atbash*-menetelmällä. Mutta on yksi *Shift* -menetelmän avain, jolla salaustulos on sama *Atbash*- ja *Shift*-menetelmien järjestyksestä riippumatta. Mikä on tämä avain? Perustele vastauksesi.

2. Olkoon f funktio, joka kuvaa kaksi 16-bittistä jonoa X ja Y kahdeksi 16-bittiseksi jonoksi $f_1(X,Y)$ ja $f_2(X,Y)$. Sen avulla määritellään funktio F, joka kuvaa neljä 16-bittistä jonoa A, B, C ja D neljäksi 16-bittiseksi jonksi A', B', C' ja D' seuraavaan tapaan:

$$\begin{aligned} A' &= f_1(A \oplus B, C \oplus D) \oplus A \\ B' &= f_1(A \oplus B, C \oplus D) \oplus B \\ C' &= f_2(A \oplus B, C \oplus D) \oplus C \\ D' &= f_2(A \oplus B, C \oplus D) \oplus D. \end{aligned}$$

   (a) (3 pist) Osoita että funktio F on itsensä käänteisfunktio.

   (b) (3 pist) Mikä iteroitu lohkosalain käyttää näin määriteltyä funktiota F parillisilla kierroksilla ja mikä silloin funktio f on?

3. (6 pist) 251 on alkuluku. Laske $\phi(2008)$.

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 satun- naislukugeneraattorin. 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?

T-79.4501 Cryptography and Data Security
EXAM
Wednesday, September 3, 2008

1. (6 pts) The *Atbash cipher* is a simple substitution cipher, which converts the order of the alphabet, that is, it encrypts A to Z, B to Y, C to X, and so on, on the English alphabet. Consider double encryption using the *Atbash cipher* and *Shift cipher* on the English alphabet. Usually these ciphers do not commute, that is, if you apply *Atbash* first and then *Shift* the result is different from what you get if you apply *Shift* first and then *Atbash*. But there is one non-zero key of the *Shift* cipher, for which the encryption result is the same in both ways. What is it? Justify your answer.

2. Suppose that f is a function which maps two 16-bit strings X and Y to two 16-bit strings $f_1(X,Y)$ and $f_2(X,Y)$. Using it, we define a function F, which maps four 16-bit strings A, B, C and D, to four 16-bit strings A', B', C' and D' as follows:

$$\begin{aligned} A' &= f_1(A \oplus B, C \oplus D) \oplus A \\ B' &= f_1(A \oplus B, C \oplus D) \oplus B \\ C' &= f_2(A \oplus B, C \oplus D) \oplus C \\ D' &= f_2(A \oplus B, C \oplus D) \oplus D. \end{aligned}$$

   (a) (3 pts) Show that the function F is its own inverse.

   (b) (3 pts) Which iterated block cipher uses such a function F at the even rounds and what is then the function f?

3. (6 pts) 251 is a prime. Calculate $\phi(2008)$.

4. (6 pts) Alice is using a toy version of the DSA signature scheme with a prime modulus $p = 43$ and generator $g = 21$ of order $q = 7$. By accident, Alice generates signatures for two different messages with the same per-message random number k. The hashes of the two signed messages are 2 and 3, and the signatures are (2, 1) and (2, 6), respectively. Determine Alice's private key.

5. (6 pts) Assume that we have two number generators as black boxes. Both generators output 64-bit numbers. One box contains a Counter Mode PRNG using IDEA encryption as E_K and with a counter of length 64 bits. The second box contains a true random number generator. The boxes look exactly the same, and the task is to determine which one is the true RNG just by examining the output of the generators. After both generators have produced about 2^{32} numbers, one has about 50% chance of being able to distinguish the generators. Explain why.