T-79.4501 Cryptography and Data Security
Tentti
28.10.2008

1. Tarkastellaan Hillin salausmenetelmää Galois'n kunnassa $GF(2^4)$ polynomilla x^4+x+1. Salausavain on 2×2-matriisi

$$\begin{pmatrix} x^2 & 1 \\ 1 & x+1 \end{pmatrix}, \text{ eli bittijonomerkintää käyttäen } \begin{pmatrix} \texttt{0100} & \texttt{0001} \\ \texttt{0001} & \texttt{0011} \end{pmatrix}.$$

   a) (3 pts) Salaa sana $(x^2, x+1) = (\texttt{0100}, \texttt{0011})$.

   b) (3 pts) Laske tulkinta-avainmatriisi.

2. Alice ja Bob käyttävät CBC salausta. Selväkieli on jono lohkoja $P_1, P_2, \ldots, P_t$ ja vastaavat salakielilohkot, jotka Alice lähettää Bobille, ovat $C_1, C_2, \ldots, C_t$. Bob vastaanottaa salakielilohkot $C'_1, C'_2, \ldots, C'_t$, joista täsmälleen yhdessä lohkossa C'_j, missä $1 \leq j < t$, on virhe. Siten $C'_i = C_i$ kaikilla $i = 1, 2, \ldots, t$, paitsi kun $i \neq j$, jolloin $C'_j \neq C_j$.

   a) (3 pts) Osoita että tulkinnan jälkeen Bobin selväkielilohkoista täsmälleen kaksi on virheellistä. Mitkä ovat virheellisten salakielilohkojen indeksit?

   b) (3 pts) Kuinka virheelliset selväkielilohkot eroavat alkuperäisistä?

3. Sun Tsu oli kiinalainen matemaatikko, joskus kolmannen ja viiden vuosisadan välillä jälkeen Kristuksen. Keksimänsä Kiinalaisen Jäännöslauseen havainnollistamiseksi hän käytti esimerkkiä

$$\begin{aligned} x &\equiv 2 \pmod 3 \\ x &\equiv 3 \pmod 5 \\ x &\equiv 2 \pmod 7. \end{aligned}$$

   a) (3 pts) Ratkaise x mod 105.

   b) (3 pts) RSA voidaan määritellä myös moduulille n joka on kolmen erisuuren alkuluvun tulo. Samoin kuin tavallisen RSA:n tapauksessa salauseksponentin e ja tulkintaeksponentin d täytyy toteuttaa kongruenssi

$$ed \equiv 1 \pmod{\phi(n)}$$

   Kun $n = 105$ ja $e = 7$, laske d.

4. (6 pts) Esitä Man-in-the-Middle hyökkäys tavallista (autentikoimatonta) Diffie-Hellman avaintenvaihtoprotokollaa vastaan.

5. (6 pts) Oletetaan että on annettu kaksi lukugeneraattoria mustina laatikkoina, eli päältäpäin ne näyttävät aivan samoilta, ja voimme ainoastaan tarkastella niiden tuottamia lukujonoja. Molemmat generaattorit tuottavat 64-bittisiä lukuja. Edelleen on annettu että toinen laatikko sisältää laskurigeneraattorin, joka käyttää Triple-DES salausta ja 64-bittistä laskuria. Toinen laatikko sisältää todellisen satunnaislukugeneraattorin. Tehtävänä on erottaa nämä laatikot toisistaan. Kun molemmat generaattorit ovat tuottaneet noin 2^{32} lukua, on noin 50% todennäköisyys, että generaattorit pystytään erottamaan. Mihin tämä perustuu?

Laskimen käyttö tentissä. Tavallinen, ei ohjelmoitava, funktiolaskin on sallittu.

T-79.4501 Cryptography and Data Security
EXAM
Tuesday, October 28, 2008

1. A Hill cipher is defined over Galois field $GF(2^4)$ with polynomial $x^4 + x + 1$. The encryption key is the 2×2-matrix

$$\begin{pmatrix} x^2 & 1 \\ 1 & x+1 \end{pmatrix}, \text{ or using bit notation } \begin{pmatrix} \texttt{0100} & \texttt{0001} \\ \texttt{0001} & \texttt{0011} \end{pmatrix}.$$

   a) (3 pts) Compute the encryption of the word $(x^2, x+1) = (\texttt{0100}, \texttt{0011})$.
   b) (3 pts) Compute the decryption key.

2. Alice and Bob use CBC encryption. The plaintext is a sequence of blocks $P_1, P_2, \ldots, P_t$ and the corresponding ciphertext blocks sent by Alice to Bob are $C_1, C_2, \ldots, C_t$. Bob receives ciphertext blocks $C'_1, C'_2, \ldots, C'_t$, where exactly one ciphertext block C'_j has an error, where $1 \leq j < t$. Then $C'_i = C_i$ for all $i = 1, 2, \ldots, t$, $i \neq j$, and $C'_j \neq C_j$.

   a) (3 pts) Show that after decryption by Bob exactly two plaintext blocks are erroneous. What are the indices of the erroneous plaintext blocks?
   b) (3 pts) How the erroneous plaintext blocks differ from the original?

3. Sun Tsu was a Chinese mathematician, sometime between the third to fifth century AD. To illustrate the Chinese Remainder Theorem he used an example

$$\begin{aligned} x &\equiv 2 \,(\mathrm{mod} 3) \\ x &\equiv 3 \,(\mathrm{mod} 5) \\ x &\equiv 2 \,(\mathrm{mod} 7) \end{aligned}$$

   a) (3 pts) Solve for x mod 105.
   b) (3 pts) RSA can also be defined for a modulus n which is a product of three different primes. Similarly as in the usual case, the encryption exponent e and the decryption exponent d must satisfy

$$ed \equiv 1 (\mathrm{mod} \phi(n)).$$

   For $n = 105$ and $e = 7$ compute d.

4. (6 pts) Explain the Man-in-the-Middle Attack on the basic (unauthenticated) Diffie-Hellman key exchange protocol.

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 Triple-DES 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.