T-79.4501 Cryptography and Data Security
2008 / EXAM
Thursday, January 10, 2008

1. (6 pts) The ciphertext

   ```
   DLVRE BIBCC SWBKW OXYQN ZVFEO OHJDI KRRNI JMEID RIJGC SQGNO CYSUD SXLVS
   YRTTI ZXFIB KQJWC SRXHB OULGX MCRPK VCJKC KRUVR OSKJO BWKCX NEIFD OGYPS
   AYVUK FEIKK XXFHD RMJOO DLFFZ BSGQC OHSAD RIWTO XGYEB ITKQQ BEGJO BOVTM
   ULFHP SWSCC OHFPN SWTQF OVZPQ DLVMO IAFTN SXJGV PEEFD RIEWC SRXKD DSUGM
   STYGB DLVEB ITKQQ BED
   ```

   was generated using the *Vigenere Shift cipher*. Use Kasiski's method to determine the keylength (period).

2. Describe by drawing a picture, or using formulas, or both

   (a) (2 pts) the encryption function of the CBC mode of operation;

   (b) (2 pts) the decryption function of the CBC mode of operation; and

   (c) (2 pts) the CBC MAC.

3. Consider the RSA cryptosystem with modulus $n = 101 \cdot 131 = 13231$.

   (a) (3 pts) A random number generator produces three random numbers: 1313, 313 and 1030. Show that only 313 is a suitable value for the public encryption exponent $e$.

   (b) (3 pts) Compute the private decryption exponent $d$ using $e = 313$.

4. (6 pts) Determine the modulus $m$, multiplier $a$ and increment $c$ of a linear congruential generator given four consecutive outputs $x_2 = 13$, $x_3 = 7$, $x_4 = 14$ and $x_5 = 9$. Determine the initial value $x_0$.

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.

T-79.4501 Tiedon salaus ja suojaus 2008 / Tentti
10.01.2008

1. (6pist) Salakieliteksti

   ```
   DLVRE BIBCC SWBKW OXYQN ZVFEO OHJDI KRRNI JMEID RIJGC SQGNO CYSUD SXLVS
   YRTTI ZXFIB KQJWC SRXHB OULGX MCRPK VCJKC KRUVR OSKJO BWKCX NEIFD OGYPS
   AYVUK FEIKK XXFHD RMJOO DLFFZ BSGQC OHSAD RIWTO XGYEB ITKQQ BEGJO BOVTM
   ULFHP SWSCC OHFPN SWTQF OVZPQ DLVMO IAFTN SXJGV PEEFD RIEWC SRXKD DSUGM
   STYGB DLVEB ITKQQ BED
   ```

   on tuotettu *Vigenèren Siirtomenetelmällä*. Anna arvio avaimen pituudelle Kasiskin menetelmän avulla.

2. Esitä piirroksen ja/tai kaavojen avulla

   (a) (2pist) datan salaus CBC käyttötavalla;

   (b) (2pist) CBC käyttötavalla salatun datan tulkinta; ja

   (c) (2pist) CBC MAC.

3. Tarkastellaan RSA salausmenetelmää, jonka moduuli on $n = 101 \cdot 131 = 13231$.

   (a) (3pist) Satunnaisgeneraattori tuottaa kolme lukua: 1313, 313 and 3010. Osoita, että näistä ainoastaan 313 soveltuu käytettäväksi julkisena salauseksponenttina $e$ tässä menetelmässä.

   (b) (3pist) Laske salauseksponenttia $e = 313$ vastaava tulkintaeksponentti $d$.

4. (6pist) Määritä moduuli $m$, kerroin $a$ ja lisäysarvo $c$ lineaariselle kongruenssigeneraattorille kun neljä peräkkäistä sen tuottamaa lukua on annettu: $x_2 = 13$, $x_3 = 7$, $x_4 = 14$ ja $x_5 = 9$. Määritä aloitusarvo $x_0$.

5. (6pist) Tarkastellaan kahta lukugeneraattoria mustina laatikkoina, jolloin nähdään vain niiden tuottamat lukujonot. Kumpikin generaattori tuottaa 64-bittisiä lukuja. Lisäksi tiedetään, että toinen mustista laatikoista sisältää laskurimoodigeneraattorin (Counter Mode PRNG), joka käyttää Triple-DES 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?