

Tentamen i Kryptologi

1DT659

2007–06–12

Lärare: Björn Victor, inst. f. informationsteknologi (tel. 070–425 0239)

Skrivtid: 8.00–13.00

Hjälpmittel: Inga.

Accessories: None.

Anvisningar: Om ni följer dessa anvisningar underlättar ni rättningen, som då kommer att gå fortare.

If you follow these instructions you make correcting the exam easier and faster.

1. Lös endast en uppgift per blad.
Only solve one problem per sheet.
2. Skriv inte på baksidan av papperet.
Do not write on the back of the paper.
3. Skriv ditt namn *och* personnummer högst upp på *varje* blad.
Write your name and personal number at the top of *every* sheet.
4. Fyll i sid 7 och lämna in den som försättsblad tillsammans med svaren.
Complete the form on page 7 and return it as cover page together with your answers.

Lycka till!!

Good luck!!

Uppgift 0

(0 poäng)

Öka dina chanser att klara tentan och få ordentligt med poäng för dina svar:

Increase your chances of passing the exam and getting good scores for your answers:

- a. Läs anvisningarna (ovan) noggrannt, och följ dem.
Read the instructions (above) carefully, and follow them.
- b. Läs uppgifterna (nedan) noggrannt innan du börjar, och lös dem sedan.
Read the problems (below) carefully before you start, and then solve them.

- (1) Motivera **alltid** dina svar. Du ska övertyga läsaren att du förstått frågan och svaret, och ska inte anta att läsaren kan svaret.
Always motivate your answers. You need to convince the reader that you have understood the question and the answer, and should not assume that the reader knows the answer already.
 - (2) Beskriv alla antaganden du gör.
Describe all assumptions you make.
 - (3) Skriv hellre för mycket och detaljerat än för litet och luddigt.
It's better to write lengthy and detailed answers, than sketchy and short.
 - (4) Rita gärna figurer!
Use figures when appropriate!
 - (5) Skriv tydligt. Oläsliga svar ger inga poäng.
Write in a clear handwriting. Illegible answers give no score.
-

Uppgift 1

(5 poäng)

- a. Ett kryptosystem definieras formellt som en 5-tupel $\langle \mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D} \rangle$. Beskriv vilka delarna är och vilka krav som ställs på dem, t.ex. i relation till varandra.
A crypto system is formally defined as a 5-tupel $\langle \mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D} \rangle$. Describe the parts and the requirements on them, e.g. in relation to eachother.
- b. För vilka av följande värden på k är $E_k(m) = m^k \bmod 41$ ett chiffer över \mathbb{Z}_{41} ? Motivera svaret!
For which of the following values of k is $E_k(m) = m^k \bmod 41$ a cipher over \mathbb{Z}_{41} ? Motivate your answer!
 - (1) $k = 3$
 - (2) $k = 5$
 - (3) $k = 7$

Uppgift 2

(2 poäng)

Definiera följande begrepp, och ge exempel på chiffer av dessa typer.

- a. *ovillkorlig* säkerhet
- b. *beräkningsmässig* säkerhet

Define the following terms, and give examples of ciphers of these types.

- a. unconditional security
- b. computational security

Uppgift 3

(2 poäng)

Kryptering i ett Vigenère-chiffer definieras som vi vet av

$$E_{k_i}(m) = (m + k_i) \bmod n$$

där n är längden på alfabetet och k_i delarna i nyckeln. Definiera nu kryptering i ett *Beaufort-chiffer* genom

$$E_{k_i}(m) = (k_i - m) \bmod n.$$

Jämför de båda med avseende på kryptering och dekryptering. Rita gärna figurer!

Encryption in a Vigenère cipher is, as we know, defined by

$$E_{k_i}(m) = (m + k_i) \bmod n$$

where n is the length of the alphabet and k_i the parts of the key. Now define encryption in a *Beaufort cipher* by

$$E_{k_i}(m) = (k_i - m) \bmod n.$$

Compare the two with respect to encryption and decryption algorithms; draw figures as you find appropriate.

Uppgift 4 (3 poäng)

a och b är *multiplikativa inverser modulo n* om $ab \bmod n = 1$. Hur kan vi med hjälp av Eulers sats hitta en invers b givet a och n ? Beskriv både det allmänna fallet och fallet då n är ett primtal.

a and b are *multiplicative inverses modulo n* if $ab \bmod n = 1$. How can we, using Euler's theorem, find an inverse b given a and n ? Describe both the general case and the case when n is a prime.

Uppgift 5 (4 poäng)

I alla kryptosystem gäller att motståndarens osäkerhet om nyckeln givet en kryptotext är minst lika stor som hennes osäkerhet om klartexten givet en kryptotext. Formulera detta uttryckt med villkorliga entropier, och visa påståendet matematiskt.

In all crypto systems it holds that the attacker's uncertainty about the key given a ciphertext is at least as big as the uncertainty about the plaintext given a ciphertext. Formulate this statement using conditional entropies, and prove the statement mathematically.

Uppgift 6 (4 poäng)

- Med "dubbel-DES", där krypteringen görs med två 56-bitars nycklar enligt $c = E_{k_1}(E_{k_2}(m))$, blir en känd-klartext-attack svårare (även med ett fåtal klartexter). Men hur mycket svårare, och varför? Motivera svaret noggrant.

Using "double DES", where the encryption is done using two 56-bit keys as $c = E_{k_1}(E_{k_2}(m))$, a known-plaintext attack is more difficult than "single DES" (even with few plaintexts). But how much harder, and why? Motivate your answer carefully.

- b. Om man använder lika många nycklar men istället trippel-DES, där $c = E_{k_1}(E_{k_2}(E_{k_1}(m)))$, hur svår blir en känd-klartext-attack då? Varför?
If you use as many keys, but instead “triple DES” where $c = E_{k_1}(E_{k_2}(E_{k_1}(m)))$, how hard is a known-plaintext attack in this case? Why?
-

Uppgift 7

(5 poäng)

Internet-protokollet IP använder en checksumma för att kontrollera att överföringen av header-fältet gått bra. Denna checksumma beräknas genom att ta ett-komplements-summan av alla 16-bits ord i header-fältet. (Detta ger ett 16-bits värde.)

Definiera begreppen *kryptografisk checksumma* och *hashfunktion*. Jämför dessa med varandra och med den typ av checksumma som används i IP. (IP-checksumman går ju t.ex. mycket snabbare att beräkna – varför behövs de andra typerna?)

The internet protocol IP uses a checksum to verify that the transmission of the header fields was OK. This checksum is computed by taking the one-complement sum of all 16-bit words in the header. (This gives a 16-bit value.)

Define the concepts *cryptographic checksum* and *hash function*. Compare and relate these to each other and to the type of checksum used in IP. (The IP checksum is, e.g., much faster to compute – why are the other types needed?)

Uppgift 8

(6 poäng)

Ett affint chiffer har som bekant

$$E_{(a,b)}(m) = (a \cdot m + b) \bmod n$$

dvs nyckeln är ett talpar (a, b) där $a < n, b < n$. Nedan använder vi $n = 26$, klartexter och kryptotexter från \mathbb{Z}_n , och låter tecknen A–Z representeras av 0–25.

An affine cipher has

$$E_{(a,b)}(m) = (a \cdot m + b) \bmod n$$

so the key is a pair (a, b) where $a < n, b < n$. Below, we use $n = 26$, $\mathbf{M} = \mathbf{C} = \mathbf{Z}_n$, and represent the characters A–Z by integers 0–25.

- a. Hur kan ett skiftchiffer definieras i termer av ett affint chiffer?
How can a shift cipher be defined in terms of an affine cipher?

- b. Givet en krypteringsnyckel (a, b) , hur sker dekryptering?
Given an encryption key (a, b) , how is decryption done?
 - c. Kryptera klartexten DES med nyckeln (3,11).
Encrypt the plaintext DES with the key (3,11).
 - d. Dekryptera kryptot KNL som krypterats med samma nyckel.
Decrypt the cipher KNL which was encrypted with the same key.
 - e. Beskriv hur en *chosen-plaintext*-attack på ett affint chiffer går till.
Describe how a chosen-plaintext attack on an affine cipher is done.
-

Uppgift 9 (4 poäng)

Beskriv noggrant fyra olika grundläggande sätt (*modes*) att använda ett blockchiffer som DES.

Give detailed descriptions of four basic modes for using a block cipher like DES.

Uppgift 10 (2 poäng)

Beräkna $31^{792} \bmod 851$. Glöm inte att redovisa beräkningen noggrant!

(Tips: $792 = 22 \cdot 36$.)

Calculate $31^{792} \bmod 851$. Don't forget to account carefully for your calculation!

(Hint: $792 = 22 \cdot 36$.)

Försättsblad för tentamen i Kryptologi (1DT659)

2007–06–12

Lämna in detta försättsblad tillsammans med svaren på frågorna.

Return this cover page together with the answers of the problems.

Jag tillåter att mitt namn och tentaresultat publiceras på webben:

I allow my name and exam result to be published on the web:

Underskrift:

Signed: _____

Namn:

Personnr:

Jag har svarat på följande uppgifter (kryssa för):

I have given solutions for the following problems (check boxes):

1.
2.
3.
4.
5.
6.
7.
8.
9.
10.

Sortera bladen innan du häftar ihop dem, snälla!

Please sort the sheets before stapling them!