

B Kommentarer till övningar

H. Wigzell. Klarar man inte av att förklara det man håller på med ska man ifrågasätta det man gör.

Detta appendix innehåller korta förslag till lösningar, bara svar eller bara anvisningar till de flesta av övningsuppgifterna. Lita inte helt blint på svaren; de kan vara behäftade med tveksamheter eller fel.

Gör seriösa försök till att själv lösa uppgifterna innan du tittar här.

OBS. DESSA FÖRSLAG ÄR TROLIGEN AV MEDIOKER KLASS!

Kapitel 1

1.1. Med den korrespondens som föreligger mellan klartexter och chiffer för ett Caesardito, nämligen

```
m a b c d e f g h i j k l m n o p q r s t u v w x y z  
c d e f g h i j k l m n o p q r s t u v w x y z a b c
```

blir klartexten: so so seam stress.

1.2. Se tex <http://www.acm.org/classics/sept95>, d v s Ken Thompsons klassiska artikel "Reflections on trusting trust".

1.3. Att det handlar om ett flödeskrypto där nyckeln återanvänds. Givet både m_i och c_i är det trivialt att härleda $k_i = m_i \mathbf{xor} c_i$. (Obs att $x \mathbf{xor} a \mathbf{xor} a = x \mathbf{xor} 0 = x$.)

1.4. Se t ex [Den90], [Sla96] eller [Sta99].

1.5. Ett nödvändigt villkor för en chifferfunktion är att den är injektiv (1 - 1). För att undersöka detta för de tre funktionerna kan man tabulera e_K -värdena för $x = 0, 1, \dots, 28$ för de tre angivna funktionerna. Resultat:

$x^2 \bmod 29$ är inte injektiv; tex är $14^2 \equiv 15^2 \equiv 22 \pmod{29}$

$x^3 \bmod 29$ är injektiv.

$x^5 \bmod 29$ är injektiv.

I kapitel 4 visas att $f: x \rightarrow x^e \bmod p$, p primtal, är injektiv precis då $\gcd(e, p - 1) = 1$.

1.6. Med $p = 5$ och $q = 7$ erhålls $\phi(n) = \phi(pq) = (p - 1)(q - 1) = 24$.

Om den privata nyckeln $d = 11$ erhålls den publika nyckeln e som lösning till

$$e d \bmod \phi(n) = 1.$$

Ekvationen $11d \bmod 24 = 1$ har lösningen $e = 11$ eftersom $11^2 \bmod 24 = 1$.

(I kapitel 4 anges generella metoder för att lösa förstgradskongruenser.)

Chiffkering av $m = 2$ enligt $c = m^e \bmod n$ ger $c = 2^{11} \bmod 35 = 2048 \bmod 35 = 18$.

Dechiffkering med $m = c^d \bmod n$ ger $m = 18^{11} \bmod 35 = 2$.

(En effektiv metod för att beräkna $a^z \bmod n$ presenteras i kapitel 4.)

1.7. Det gäller att $c_i = m_i \mathbf{xor} k_i$.

Utgå från det givna chiffret

$$c_1 \dots c_{i-1} c_i c_{i+1} \dots \quad (1)$$

Här stryks c_i och erhålls

$$c_1 \dots c_{i-1} c_{i+1} \dots \quad (2)$$

Dechiffkering ger

$$m_1 \dots m_{i-1} m_{i+1} \dots \quad (3)$$

Återchiffkering med ursprungliga k_i ger

$$c_1 \dots c_{i-1} c_i' c_{i+1}' \dots \quad (4)$$

där

$$\begin{aligned} c_i' &= m_{i+1} \mathbf{xor} k_i \\ c_{i+1}' &= m_{i+2} \mathbf{xor} k_{i+1} \\ &\dots \end{aligned}$$

Påståendet att k_j och m_j kan beräknas för $j \geq i$ om m_i är känt följer som så:

Bilda vänsterledet nedan och räkna ut.

$$c_i \mathbf{xor} c_i' = m_i \mathbf{xor} k_i \mathbf{xor} m_{i+1} \mathbf{xor} k_i = m_i \mathbf{xor} m_{i+1}.$$

Ur detta kan lösas ut $m_{i+1} = m_i \mathbf{xor} c_i \mathbf{xor} c_i' =$ kända/observerade kvantiteter.

När denna klartext är känd kan nyckeln beräknas: $k_{i+1} = m_{i+1} \mathbf{xor} c_{i+1}$.

Ett induktionsbevis är nu enkelt att utföra.

1.8. Med given nyckelrestriktion finns det bara $26^7 \approx 10^{10}$ möjligheter. Uttömmande nyckelsökning tar då $10^{10} \mu\text{s} = 10^4 \text{ sek} \approx 3$ timmar.

Med $2^{56} \approx 10^{17}$ nycklar blir resultatet ca 10^6 dagar.

1.9. Antag att CBC producerar y_1, \dots, y_n och att CFB producerar z_1, \dots, z_{n-1} .

Det är "lätt" att inse att $y_{i+1} = e_K(z_i)$. Tag $i = n - 1$ så följer påståendet.

1.10. Det är sant, ty om $r \equiv 0 \pmod{4}$ eller $r \equiv 2 \pmod{4}$, så är r inte ett primtal.

1.11. $\log_2 8^{130} = 130 * \log_2 8 = 130 * \log_2 2^3 = 130 * 3 = 390$.

De vanliga logaritmlagarna är:

- a. $\log x^y = y \log x$.
 - b. $\log x y = \log x + \log y$.
 - c. $\log x / y = \log x - \log y$.
 - d. $\log 1 / x = -\log x$. (ett specialfall av c.)
-

1.12. Om x är udda kan det skrivas $x = 2u + 1$. Då blir $x^2 = (2u + 1)^2 = 4u^2 + 4u + 1 = 4u(u + 1) + 1 = z + 1$.

Men $u(u + 1)$ är jämnt för alla u eftersom endera u eller $u + 1$ är jämnt.

Alltså är z jämnt delbart med $2 * 4 = 8$ och $x^2 \equiv 1 \pmod{8}$.

1.13. Kvantiteten H blir

$$H = 3 * 1/4 \log 4 + 1/8 \log 8 + 2 * 1/16 \log 16 = 2/4 + 3/8 + 4/16 = 2 3/8.$$

Entropiolikheter tex $0 \leq H \leq \log n$ behandlas i kapitel 3.

1.14. Följande "definitioner" av attacker är aktuella:

- Endast-nyckel: Motståndaren känner bara till den öppna nyckeln och kan alltså endast verifiera signaturer.

- Känd-signatur: Motståndaren känner till den öppna nyckeln och har observerat ett antal autentiska par <meddelande, signatur>

- Vald-klartext: Motståndaren känner till den öppna nyckeln och tillåts att be om ett antal par <meddelande, signatur>, där motståndaren kan välja meddelanden.

Motståndaren kan forcera genom

- Existensiellt bedrägeri: Motståndaren lyckas att skapa en signatur på ett meddelande.

- Selektivt bedrägeri: Motståndaren lyckas skapa en korrekt signatur på ett valt meddelande.

- Universellt bedrägeri: Motståndaren lyckas att skapa korrekta signaturer på godtyckliga meddelanden utan att för den skull ha lyckats bestämma den privata nyckeln.

- 'Total break': Motståndaren har lyckats härleda den privata nyckeln.

1.15. Ett block för ECB och OFB, två block för CBC och CFB.

Kapitel 2

2.1. Givet $c_0 = 1001$ erhålls med CBC, där e är given permutation att

$$c_1 = e(m_1 \mathbf{xor} c_0) = e(0001 \mathbf{xor} 1001) = e(1000) = 0100.$$

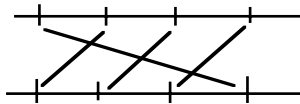
$$c_2 = e(m_2 \mathbf{xor} c_1) = e(1110 \mathbf{xor} 0100) = e(1010) = 0101.$$

Återchiffreeringen sker med

$$m_1 = e^{-1}(c_1) \mathbf{xor} c_0 = 1000 \mathbf{xor} 1001 = 0001. \quad (\text{stämmer})$$

$$m_2 = e^{-1}(c_2) \mathbf{xor} c_1 = 1010 \mathbf{xor} 0100 = 1110. \quad (\text{stämmer})$$

Notera att e^{-1} definieras av $\langle 1, 2, 3, 4 \rangle \rightarrow \langle 2, 3, 4, 1 \rangle$



2.2. I ett Vigenèrechiffer med nyckellängd 5 kommer var 5:te symbol att chifferas med samma nyckel, tex symbolerna nummer 1 och 6.

I chiffret j o z m n y är den numeriska skillnaden mellan j och y lika med 15.

Då gäller samma skillnad för den riktiga klartexten.

DALLAS ger S - D = 15.

AUSTIN ger N - A = 13.

Klartexten är alltså DALLAS.

2.3. Vigenère, igen.

Chiffer	yfn	gfm	ikk	ixa	t	
Nyckel	art	art	art	art	t	You got it right !
Klartext	you	got	itr	igh	t	

2.4. I ett Hillchiffer gäller $\mathbf{m} = \mathbf{H}^{-1} \mathbf{c}$ (här underförstått *mod* 26). Här är högerledet givet. Alltså blir

$$\mathbf{m} = \begin{vmatrix} 15 & 20 \\ 17 & 9 \end{vmatrix} \begin{vmatrix} 11 \\ 9 \end{vmatrix} = \begin{vmatrix} 7 \\ 8 \end{vmatrix} \begin{matrix} \text{-- G} \\ \text{-- H} \end{matrix}$$

2.5. Chiffret är av typen $c = am + b \pmod{26}$ och notera:

$\begin{array}{c} c \quad m \\ \hline F \quad E \\ W \quad H \end{array}$	numeriskt	$\begin{array}{c} c \quad m \\ \hline 5 \quad 4 \\ 22 \quad 8 \end{array}$
---	-----------	--

Detta ger upphov till ekvationssystemet ($\pmod{26}$)

$$\begin{aligned} 5 &= 4a + b \\ 22 &= 7a + b. \end{aligned}$$

Subtrahera den första ekvationen från den andra. Det ger följande.

$$3a \equiv 17 \pmod{26}.$$

Lös denna ekvation (på något sätt). Lösningen är $a = 23 (= X)$

Konstanten b erhålls med hjälp av första ekvationen.

$$b \equiv 5 - 4a \equiv 5 - 92 \equiv -87 \equiv 17 \pmod{26}.$$

Det affina chiffret är alltså

$$c = 23m + 17 \pmod{26}.$$

2.6. Här gäller

$$\begin{aligned} m &= 100\ 011 \\ c &= 101\ 101 \end{aligned}$$

och alltså

$$k = 001\ 110.$$

Ekvationen $\mathbf{Y} = \mathbf{H} \mathbf{X} \pmod{2}$ blir alltså

$$\begin{vmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{vmatrix} = \begin{vmatrix} t_3 & t_2 & t_1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{vmatrix} * \begin{vmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{vmatrix}$$

Räkna ut första raden i högerledet och identifiera den med första raden i vänsterledet:

$$\begin{aligned} t_3 = 1 &\Rightarrow t_3 = 1 \\ t_3 + t_2 = 1 &\Rightarrow t_2 = 0 \\ t_3 + t_2 + t_1 = 0 &\Rightarrow t_1 = 1 \end{aligned}$$

Avtappingsvektorn är alltså $\mathbf{T} = \langle 1, 0, 1 \rangle$. Kontrollera gärna att denna ger angivet chiffer.

2.7. Inget svar här.

2.8. Två chiffer över Z_n är givna.

$$S_1: y = Hx \qquad S_2: y = x + k$$

$$S_1 S_2 \text{ ger } S_1(x + k) = H(x + k) = Hx + Hk = Hx + k'.$$

$$S_2 S_1 \text{ ger } S_2(Hx) = Hx + k.$$

2.9. I varje varv finns två **xor**-operationer; en då funktionen f bildas och en i samband med höger/vänsterutbytet.

- Om klartexten och nyckeln byter polaritet så kommer f att bli opåverkad; det gäller ju att $a \text{ xor } b = \text{not } a \text{ xor not } b$.

- I utbytesfasen komplementeras bara en operand i **xor**-operationen. Då komplementeras resultatet; det gäller ju att $\text{not } (a \text{ xor } b) = \text{not } a \text{ xor } b$.

Slutsatsen följer av att detta upprepas 16 gånger och att DES i övrigt bara innehåller permutationer och substitutioner.

De båda **xor**-ekvationerna visas enkast via sanningstabeller. (Operationen **not** har precedens över **xor**.)

2.10. Följande chiffer är givna.

$$M: y = ax \text{ mod } 26, \text{ där } \gcd(a, 26) = 1, \text{ så } |\mathbb{K}| = \phi(26) = 12.$$

$$S: y = x + b \text{ mod } 26, \text{ där } b = 0, \dots, 25, \text{ så } |\mathbb{K}| = 26.$$

$$\text{Produkten } M S \text{ blir } y = M(x + b) \text{ mod } 26 = ax + ab \text{ mod } 26.$$

Alla ab i $[0, 25]$ och därmed alla b är användbara.

$$\text{Däremot måste } a \in \mathbb{Z}_{26}^* \Rightarrow |\mathbb{K}| = 12 * 26 = 312.$$

$$\text{Produkten } S M \text{ blir } y = S(ax \text{ mod } 26) = ax + b \text{ mod } 26.$$

$$\text{Alla } b \text{ i } [0, 25] \text{ är användbara. Däremot måste } a \in \mathbb{Z}_{26}^* \Rightarrow |\mathbb{K}| = 12 * 26 = 312.$$

2.11. Kvadratuträkning ger (kom ihåg att $(a - b)^2 = a^2 - 2ab + b^2$!)

$$\sum_i (p_i - 1/26)^2 = \sum_i p_i^2 - 2 \sum_i p_i / 26 + \sum_i (1/26)^2 = \sum_i p_i^2 - 1/13 + 1/26.$$

Alltså:

$$\sum_i p_i^2 = \sum_i (p_i - 1/26)^2 + 1/26 \geq \{\text{en kvadrat är icke-negativ}\} \geq 1/26.$$

2.12. Registrets initialtillstånd ges uppenbarligen av 00001 eftersom detta tappas av utan modifikation. Kvar är att bestämma avtappningssekvensen $T = \langle t_5, \dots, t_1 \rangle$.

2.13. Ja, ty om den högraste cellen inte påverkar återkopplingen, så kan man ta bort den och därmed förkorta registret. Ett $n - 1$ bits LFSR kan inte ge en period längre än $2^n - 1$, som är mindre än $2^n - 1$.

2.14. Roligt att du kan läsa, skriva och tala som alla andra bland oss här i Uppsala.

2.15. Här gäller att $e_k(5, 17) = (15, 16)$, $e_k(8, 3) = (2, 5)$, ..., och $e_k(0, 24) = (10, 20)$.

Ur de två första paren följer att $(\mathbf{Y} = \mathbf{X} \mathbf{K})$

$$\begin{vmatrix} 15 & 16 \\ 2 & 5 \end{vmatrix} = \begin{vmatrix} 5 & 17 \\ 8 & 3 \end{vmatrix} * \mathbf{K}$$

\mathbf{X} inverteras och därefter bildas $\mathbf{K} = \mathbf{X}^{-1} \mathbf{Y}$, som ger

$$\mathbf{K} = \begin{vmatrix} 7 & 19 \\ 8 & 3 \end{vmatrix}$$

Detta resultat kan verifieras mot det tredje $\langle x, y \rangle$ -paret.

2.16. Med $y = 2x \pmod{26}$ erhåller vi (översatt till bokstäver)

$$\begin{aligned} x &= a b c d e f g h i j k l m n o p q r s t u v w x y z \\ y &= b d f h j l n p r t v x z b d f h j l n p r t v x z \end{aligned}$$

Alternativt: Eftersom $\text{gcd}(2, 26) = 2$ har ekvationen $y = 2x \pmod{26}$ två lösningar m a p x .

2.17. Inget svar här.

2.18. Om $b \neq c$ men $b(2b + 1) = c(2c + 1) \pmod{2^w}$ så är $(b - c)(2b + 2c + 1) = 0 \pmod{2^w}$. Men $b - c$ är nollskiljt och $2b + 2c + 1$ är udda. Produkten kan då inte vara $0 \pmod{2^w}$.

Kapitel 3

3.1. Dela upp entropin i två delsummer.

$$H_1 = \sum_{0 \leq i \leq 255} 1 / (2 * 256) \log 2 * 256 = 4.5.$$

$$H_2 = \sum_{i > 255} 1 / (2 * (2^{32} - 2^9)) \log 2 * (2^{32} - 2^9) = 1/2 \log (2^{33} - 2^{10}) \approx$$

$$1/2 \log 2^{33} = 16.5. \quad (2^{10} \text{ är "löjligt lite", } < 1 \text{ promille, relativt } 2^{33}.)$$

Entropin $H = H_1 + H_2$ blir därför 21, cirka.

$$\begin{aligned} 3.2. H(X) = & 1/4 \log 4 + 1/4 \log 4 + 1/4 \log 4 + \\ & 1/8 \log 8 + \\ & 1/16 \log 16 + 1/16 \log 16 = 2 \frac{3}{8}. \end{aligned}$$

Huffmankodning ger

<i>a</i>	-	00
<i>b</i>	-	01
<i>c</i>	-	10
<i>d</i>	-	110
<i>e</i>	-	1110
<i>f</i>	-	1111

Medelkodordslängden blir $2 \frac{3}{8}$, dvs lika med entropin. (Varför?)

3.3. För $n = 2$ blir entropifunktionen $H(X) = -p_1 \log p_1 - p_2 \log p_2$.

Nu är förstås $p_1 + p_2 = 1$ så om vi skriver $p_1 = p$ så blir $p_2 = 1 - p$. Funktionen blir därför

$$H(X) = -p \log p - (1 - p) \log (1 - p) = h(p).$$

Derivera för att finna extrempunkt.

$$\begin{aligned} -dh/dp &= 1 * \log p + p * 1/p + (-1) \log (1 - p) + (1 - p) / (1 - p) (-1) = \\ &= \log p + 1 - \log (1 - p) - 1 = \log p - \log (1 - p). \end{aligned}$$

Derivatans nollpunkt är $p = 1 - p$, dvs $p = 1/2$, så $p = 1/2$ är en extrempunkt.

$$d^2h/dp^2 = - [1/p + 1 / (1 - p)] \leq 0 \text{ för } 0 < p < 1.$$

Vidare är $h(0) = h(1) = 0$ och $h > 0$ för övrigt. Alltså maximum.

3.4. Lösningen finns i texten.

3.5. $H(X, Y) - H(X) - H(Y) =$

$$= -\sum_{x,y} p(x, y) \log p(x, y) + \sum_x p(x) \log p(x) + \sum_y p(y) \log p(y) =$$

= {sätt in $p(x) = \sum_y p(x, y)$ och $p(y) = \sum_x p(x, y)$ efter summatecknet i de två sista termerna och bryt ut} =

$$= \sum_{x,y} p(x, y) [\log p(x) + \log p(y) - \log p(x, y)] = \sum_{x,y} p(x, y) \log [p(x) p(y) / p(x, y)] \leq$$

$$\{ \text{använd nu it-olikheten} \} \leq \sum_{x,y} [p(x) p(y) / p(x, y) - 1] \log e =$$

$$\log e [\sum_{x,y} p(x) p(y) - \sum_{x,y} p(x, y)] = \log e [\sum_x p(x) \sum_y p(y) - 1] = 0.$$

3.6. Redan visat i texten.

3.7. Alla M och K är lika sannolika och $0 \leq K \leq 9$ enligt förutsättningar. Det gäller att:

$$H(M) = \log 10^6 \approx 19.2$$

$H(C) = H(M)$, ty alla chiffer bli lika sannolika.

$$H(K) = \log 10 \approx 3.3.$$

$H(M|C) = \log 10$, eftersom det finns 10 möjliga nycklar.

$$H(K|C) = \log 10.$$

3.8. $I(X, Y) = \{\text{givet}\} = \sum_{x, y} p(x, y) \log (p(x|y) / p(x)) = \{\text{logaritmlag}\} =$
 $= \sum_{x, y} p(x, y) \log p(x|y) - \sum_{x, y} p(x, y) \log p(x) = \{\text{definition av ekvivokation}\} =$
 $= -H(X|Y) - \sum_{x, y} p(x, y) \log p(x) = \{p(x) = \sum_y p(x, y) \text{ \& definition av entropi}\} =$
 $= H(X) - H(X|Y).$

3.9. Frågan innebär att följande summa skall beräknas.

$$\sum_{i \geq 1} i / 2^i = 1/2 + 2/4 + 3/8 + 4/16 + 5/32 + \dots \quad (1)$$

Den påminner lite om en geometrisk serie så börja med att studera

$$f(x) = \sum 1/x^i. \quad (2)$$

Om $|x| < 1$ konvergerar denna och kan beräknas med en sluten formel.

$$f(x) = 1 / (x - 1).$$

Derivering ger att

$$f'(x) = -1 / (x - 1)^2. \quad (3)$$

Denna derivata kan emellertid också erhållas från (2):

$$f'(x) = -1/x^2 - 2/x^3 - 3/x^4 - \dots = \{\text{som vi skriver}\} = -1/x [1/x + 2/x^2 + \dots] =$$
$$= -g(x)/x \quad (4)$$

med

$$g(x) = 1/x + 2/x^2 + 3/x^3 + \dots \quad (5)$$

Ekvationerna (3) och (4) ger

$$g(x) = x / (x - 1)^2. \quad (6)$$

Men med $x = 2$ i (5) erhålls serien (1).

Värdet $g(2)$ är nu enkelt att beräkna via (6).

Slutsats. Entropin = 2.

3.10. Givna data ger direkt att

$$H(M) = 1/2 \log 2 + 1/3 \log 3 + 1/6 \log 6 \approx 1.459$$

För att beräkna $H(C)$ behövs $p(c)$ - chifferdistributionen; se tex 3.5.4.ii.

$$\begin{aligned} p(1) &= p(k_1) p(a) + p(k_3) p(c) = 2/9. \\ p(2) &= p(k_1) p(b) + p(k_2) p(a) = 5/18. \\ p(3) &= p(k_1) p(c) + p(k_2) p(b) + p(k_3) p(a) = 1/3. \\ p(4) &= p(k_2) p(c) + p(k_3) p(b) = 1/6. \end{aligned}$$

Detta ger

$$H(C) \approx 1.955.$$

Att beräkna $H(K)$ är enkelt eftersom nyckeldistributionen är känd.

$$H(K) \approx 1.585.$$

För att beräkna $H(K | C)$ används lämpligen satsen i avsnitt 3.5.2.iii

$$H(K | C) = H(K) + H(M) - H(C) \approx 1.089.$$

För att beräkna $H(M | C)$ finns två alternativ:

- Använd definitionen direkt föregående av bestämning av $p(m | c)$, JOBBIGT ! Detta ger dock resultatet $H(M | C) \approx 1.089$.
- Ovanstående resultat liknar $H(K | C)$. Är de lika ?

Använd nu det kända sambandet $H(X, Y) = H(Y) + H(X | Y)$ och beviset av satsen 3.5.2.iii och räkna lite.

$$\begin{aligned} H(M | C) &= H(M, C) - H(C) = H(K, M, C) - H(K | M, C) - H(C) = \\ &= H(K) + H(M) - H(K | M, C) - H(C) = \\ &= H(K | C) - H(K | M, C). \end{aligned}$$

$$\text{Notera: } H(M | C) = H(K | C) - H(K | M, C) \rightarrow H(K | C) \geq H(M | C) \quad (*)$$

I detta exempel är emellertid $H(K | M, C) = 0$ eftersom om både klartext och chiffer är givna så är nyckeln entydigt bestämd.

Anmärkning. Ovanstående entropiräkning (*) ger även svaret på frågan 3.17.

3.11. Om en tärning slås en gång är sannolikheten att en sexa inte uppträder $5/6$.

Om en tärning slås 10 gånger är sannolikheten att en sexa inte uppträder någon gång $(5/6)^{10}$.

Alltså är sannolikheten att en sexa uppträder minst en gång $1 - (5/6)^{10}$.

3.12. Använd approximationen $N_u = H(K) / D$.

Affint chiffer. Om $K \in Z_n^* \times Z_n$ så blir $H(K) = \log n\phi(n)$.

Permutation. Det finns $d!$ sådana varför $H(K) = \log d! \approx d \log d$. (Stirlings formel.)

3.13. En bridgehand om 13 kort kan väljas ut på $x = 52! / 13! (52 - 13)!$ olika sätt ur en kortlek om 52 kort. Den maximala ovissheten är då $\log x \approx 52 h(1/4)$. (Stirlings formel, igen.), ty

$$\log((n, k)) \approx n [k/n \log n/k + (n - k)/n \log n/(n - k)] = n h(k/n).$$

3.14. a. $R = \log L$, där $L = 4$ i detta fall. Alltså $R = 2$.

Med givna sannolikheter erhålls $H(M) = 1 \frac{3}{4}$; detta är 0-te ordningens approximation för hastigheten r . Vidare är $D = R - r = 1/4$.

b. Med digram som grundsymboler fås $R = \log 16 = 4$.
Angivna sannolikheter ger $H(X, Y) = 7.5$, varför $r = 3.75$ och alltså $D = 1/4$.

3.15. Räkna analogt med motsvarande bevis för skiftchiffer.

3.16. a. Chiffermatrisen blir

	1	2	3
k_1	1	2	3
k_2	0	1	2
k_3	0	3	2

b. I chiffret förekommer chiffersymbolerna 0, 2 och 3. Det gör att varken k_1 eller k_2 har kunnat användas.

3.17. Se lösningen på uppgift 3.10.

3.18. Tanken är att utnyttja approximationen $H(K | C)_N = H(K) - DN$.

Om man ritat f som en funktion av N med givna data erhålls en rät linje med riktningskoefficient $= -(64 - 49) / 5 = -(49 - 34) / 5 = -3$.

Ur detta inses att $D = 3$. Vidare är $H(K) = H(C | K)_{N=0} = 64$.

Entydighetslängden är den punkt på N -axeln som skärs av den räta linjen, dvs $N_u = H(K) / D = 21 \frac{1}{3}$.

3.19. Med hjälp av både klartext och chiffer är nyckeln entydigt bestämd. $H(K | M, C) = 0$.

3.20. Hoppa gärna över denna övning.

3.21. $H = \sum_{n \in [0,56]} p_n \log 1/p_n$, där $p_n = \binom{56}{n} / 2^{56}$, så $H \approx 3.95$.

($\binom{.}{.}$) är binomialkoefficienten.

3.22. Javisst!

3.23.

Räkna med $N_u = H(K) / D$ och svara (ofullständigt) med följande tabell.

Chiffer	$H(K)$
Caesar	$\log 26 \approx 4.7$
Allmän substitution	$\log n! \approx n \log n$
Vigenere	$\log 26^{\text{period}} = 4.7 * \text{period}$
Affina	$\log 26 * \phi(26) = \log 312$
LFSR	$\log 2^{\text{period}} = \text{period}$
Rotor	$\log 26^t = 4.7 * t$
DES	$\log 2^{56} = 56$
Skipjack	$\log 2^{80} = 80$
Pohlig-Hellman	$\log \phi(\phi(p)) = \log \phi(p - 1)$
IDEA	$\log 2^{128} = 128$
OTP	∞
PKS	0

Kapitel 4

4.1. Använd sambandet $\phi(n) = \prod_i p_i^{e_i-1} (p_i - 1)$. Talet $p_i - 1$ är jämnt (om $p_i > 2$).

4.2. Bestäm $7^{1000} \pmod{10}$. Eftersom $\gcd(7, 10) = 1$ kan Eulers sats $a^{\phi(m)} \equiv 1 \pmod{m}$ användas med $a = 7$ och $m = 10$. $\phi(10) = \phi(2 * 5) = (2 - 1) * (5 - 1) = 4$.

Detta ger $7^4 \equiv 1 \pmod{10}$ och $7^{1000} \equiv (7^4)^{250} \equiv 1 \pmod{10}$. Entalssiffran är alltså 1.

4.3. Talet n kan skrivas

$$n = d_1 10^{t-1} + d_2 10^{t-2} + \dots + d_{t-1} 10 + d_t.$$

Bilda $n \pmod{9}$ och observera att $10 \pmod{9} = 1$ och att $d_i \pmod{9} = d_i$ eller 0. Då erhålls

$$n \bmod 9 = (d_1 + \dots + d_t) \bmod 9.$$

Anmärkning. Resultatet kan användas för att enkelt avgöra om ett tal är delbart med 9. Det finns en liknande relation för modulen 11. Hur ser den ut ?

4.4. a. $5x \bmod 17 = 1$ är given. Ekvationen har en entydig lösning eftersom $\gcd(5, 17) = 1$. Euklides algoritm ger

i	g	v	y	
0	17	0	-	Alltså $x = 7$. Kontrollera gärna att $5 * 7 \bmod 17 = 1$.
1	5	1	3	
2	2	-3	2	
3	1	<u>7</u>	1	
4	0			

Eftersom 17 är ett primtal kan man också räkna ut $x = 5^{17-2} \bmod 17$.

b. $19x \bmod 26 = 5$ är given. Ekvationen har en entydig lösning eftersom $\gcd(19, 26) = 1$.

Vi börjar med att lösa $19y \bmod 26 = 1$ med Euklides algoritm och finner $y = 11$.

Lösningen x är därför $x = 5y \bmod 26 = 3$.

c. $15x \bmod 25 = 10$. Här gäller $\gcd(15, 25) = 5$ och $5 \mid 10$. Alltså finns fem lösningar.

Lös först ekvationen $15/5 y \bmod 25/5 = 1$, dvs $3y \bmod 5 = 1$. Lösningen är $y = 2$.

Därefter tar vi fram lösningen till $3z \bmod 5 = 2$; $z = 4$.

Så lösningarna till $15x \bmod 25 = 10$ är då $x = 4, 9, 14, 19, 24$.

4.5. Nej, ty om $f(x) = y$ så är $x = f^{-1}(y)$. Men $f(y) = f(f(x)) = x$ så alltså $f^{-1}(y) = f(y)$.

f^{-1} kan inte vara svår och lätt på samma gång.

4.6. 17 är ett primtal och $17 = 2*2*2 + 1$. Ett tal a i $\mathbb{Z}_{17} - \{0\}$ är ett primitivt element precis då $a^{16/2} \bmod 17 \neq 1$ och det finns $\phi(17-1) = 8$ primitiva element.

Man kan använda relationen $a^8 \bmod 17 \neq 1$ och kontrollera alla $a = 1, \dots, 16$ för att finna att $a = 3, 5, 6, 7, 10, 11, 12, 14$ är primitiva element.

Alternativt kan man bestämma de kvadratiske residuerna mod 17, dvs

$$\{a^2 \bmod 17 : a = 1, \dots, 16\} = \{1, 2, 4, 8, 9, 13, 15, 16\}.$$

Det är precis dessa som INTE är primitiva rötter (4.3.4.ix).

4.7. Se 4.6.

$$\begin{aligned} 4.8. \quad 2x \equiv 3 \pmod{7} &\Leftrightarrow x \equiv 5 \pmod{7} \\ 3x \equiv 0 \pmod{5} &\Leftrightarrow x \equiv 0 \equiv 5 \pmod{5} \end{aligned}$$

Enligt CRT är då $x \equiv 5 \pmod{35}$, dvs $x = 5, 40, 75, \dots$

4.9. Om x är udda gäller $x = 2k + 1$, där k är något heltal.

Då blir $x^2 = 4k^2 + 4k + 1$.

Talet $4k^2 + 4k = 4k(k + 1)$ är delbart med 8 eftersom endera av k eller $k + 1$ är jämnt.

Alltså $x \equiv 1 \pmod{8}$.

4.10. Förutsättningen är $a^{(n-1)/2} \equiv 3 \pmod{n}$ och $n > 10$.

Då gäller $a^{n-1} \equiv 3^2 \equiv 9 \pmod{n}$.

Eftersom $n > 10$ så är då $a^{n-1} \not\equiv 1 \pmod{n}$. Talet a är alltså sammansatt.

4.11. Testkör ditt program. Om det blir något annat än 0 eller 1 är programmet felaktigt.

$$4.12. \quad (p-1)! \equiv -1 \pmod{p} \quad \Leftrightarrow \quad p \text{ är ett primtal.}$$

Antag p är ett primtal. För $p = 2$ inses direkt att $(p-1)! \equiv -1 \pmod{p}$.

Med $p > 2$ givet och det faktum att $ax \equiv 1 \pmod{p}$ alltid har lösning så kan vi gruppera produkten $P = 2 * 3 * \dots * (p-2)$ parvis (det blir $(p-3)/2$ stycken par) så att vi inser att denna produkt $P \equiv 1 \pmod{p}$.

För att hantera "randvärdena" 1 och $p-1$ behövs följande lemma.

Lemma. Om p är ett primtal så är a sin egen multiplikativa invers modulo p om och endast om $a \equiv 1 \pmod{p}$ eller $a \equiv -1 \pmod{p}$.

Bevis. Om $a \equiv 1 \pmod{p}$ eller $a \equiv -1 \pmod{p}$ så inses direkt att $a^2 \equiv 1 \pmod{p}$.

Om $a^2 \equiv 1 \pmod{p}$, så gäller $p \mid (a^2 - 1)$. Eftersom $a^2 - 1 = (a+1)(a-1)$ så gäller att $p \mid a+1$ eller $p \mid a-1$. Alltså $a \equiv 1 \pmod{p}$ eller $a \equiv -1 \pmod{p}$. ♥

Nu är det bara att multiplicera P med $(p-1)$ för att finna att $(p-1)! \equiv -1 \pmod{p}$.

Antag att $(n-1)! \equiv -1 \pmod{n}$ och att n är sammansatt $n = ab$, där $1 < a, b < n$.

Men då $a < n$ inses att $a \mid (n-1)!$

Eftersom $(n-1)! \equiv -1 \pmod{n}$ så följer att $n \mid ((n-1)! + 1)$.

Det betyder att $a \mid ((n-1)! + 1)$.

Men det gäller ju också att $a \mid (n-1)!$

Alltså måste $a = 1$. Motsägelse.

Slutligen: Detta är dock en mycket beräkningskrävande primtalstest!

4.13. $x^2 \equiv 4 \pmod{77}$. Lös paret $x^2 \equiv 4 \pmod{7}$ och $x^2 \equiv 4 \pmod{11}$.

Eftersom för både 7 och 11 vi har att $7 \equiv 11 \equiv 3 \pmod{4}$ blir ekvationerna lätta att lösa

$$x \equiv 4^{(7+1)/4} \equiv 4^2 \equiv 16 \equiv 2 \pmod{7} \text{ och } x \equiv 5 \pmod{7}$$

respektive

$$x \equiv 4^{(11+1)/4} \equiv 4^3 \equiv 64 \equiv 9 \pmod{11} \text{ och } x \equiv 2 \pmod{11}.$$

Med CRT kan man kombinera dessa lösningar till lösningar modulo 77:

Par 1: $x \equiv 2 \pmod{7}$ ger $x = 2 * 11 * 2 + 9 * 7 * 8 = 9 \pmod{77}$.
 $x \equiv 9 \pmod{11}$

Par 2: $x \equiv 2 \pmod{7}$ ger $x = 2$; ses direkt.
 $x \equiv 2 \pmod{11}$

Par 3: $x \equiv 5 \pmod{7}$ ger $x = 75 (= 77 - 2)$.
 $x \equiv 9 \pmod{11}$

Par 4: $x \equiv 5 \pmod{7}$ ger $x = 5 * 11 * 2 + 2 * 7 * 8 = 68 (= 77 - 9)$.
 $x \equiv 2 \pmod{11}$

4.14. Är det inte tillräckligt med ledning i uppgiften ?

4.15. a. $\alpha = 4$.

b. Om de första nio siffrorna är korrekta så ska checksumman vara X .
Annars är det inte heller ett korrekt ISBN.

c. $-10x_{10} \pmod{11} = 11x_{10} - 10x_{10} \pmod{11} = x_{10}$.

4.16. Ett 50 bitars tal är av storlek $2^{50} \approx 10^{15}$. I intervallet $[10^{14}, 10^{15}]$ finns det cirka 10^{15} tal. Av dessa är enligt primtalssatsen

$$10^{15} / \ln 10^{15} - 10^{14} / \ln 10^{14} \approx 10^{15} / 50 - 10^{14} / 50 \approx 2 \cdot 10^{13} \text{ primtal.}$$

Andelen primtal bland de udda talen (du testar förstås inte jämna tal) blir

$$2 * 10^{13} / 0.5 * 10^{15} \approx 4 / 100.$$

Du behöver alltså testa ungefär 25 udda tal innan du finner ett primtal av denna storlek.

4.17. Notera först att $\gcd(a, b) = d$ precis då a är en multipel och d och b är en multipel av d och $\gcd(a/d, b/d) = 1$. Sannolikheten att ett slumpmässigt valt tal a är en multipel av d är precis $1/d$. Det betyder att sannolikheten för att $\gcd(a, b) = d$ är P/d^2 , där $P =$ sannolikheten att $\gcd(a, b) = 1$. Vidare gäller att $1 = \sum_{d \geq 1} \text{prob}(\gcd(a, b) = d) = \sum_{d \geq 1} P/d^2 = P \sum_{d \geq 1} 1/d^2 = P * (\pi^2/6)$. Alltså är $P = 6/\pi^2 \approx 0.6$.

Kapitel 5

5.1. Inled med

$$\begin{aligned}k_1 &= 2^d \bmod n = m_1 \mathbf{xOR} c_1 \\k_2 &= 3^d \bmod n = m_2 \mathbf{xOR} c_2\end{aligned}$$

Då erhålls:

$$\begin{aligned}k_3 &= 4^d \bmod n = 2^d 2^d \bmod n = k_1 k_1 \bmod n \\k_5 &= 6^d \bmod n = 2^d 3^d \bmod n = k_1 k_2 \bmod n,\end{aligned}$$

vilket skulle visas.

Vidare: k_m kan bestämmas om primtalsfaktoriseringen av $m = p_1 \dots p_r$ är känd och k_j är kända för $j = 1, 2, \dots, r$.

5.2. Detta är (nästan) en direkt tillämpning på 5.1.2.viii.

- a. Detta är inget RSA-system eftersom $\gcd(e, \phi(n)) > 1$, ty $\phi(n) = 24$.
 - b. Detta är inget RSA-system eftersom $\gcd(e, \phi(n)) > 1$.
 - c. $[1 + \gcd(e - 1, p - 1)] * [1 + \gcd(e - 1, q - 1)] = 15$.
 - d. $[1 + \gcd(e - 1, p - 1)] * [1 + \gcd(e - 1, q - 1)] = 21$.
-

5.3. Jodå, teorin fungerar (prova), men förslaget är onödigt omständligt och inte säkrare (beräkningsmässigt) än en vanlig RSA.

5.4. I ElGamals chiffer bestäms kryptogrammet som paret $\langle y_1, y_2 \rangle$, där

$$\begin{aligned}y_1 &= \alpha^k \bmod p = 2^3 \bmod 23 = 8. \\y_2 &= x\beta^k \bmod p = 5 * 6^3 \bmod 23 = 22.\end{aligned}$$

5.5. a. Antalet fixpunkter är $[1 + \gcd(2, p - 1)] * [1 + \gcd(2, q - 1)]$, dvs 9 fixpunkter eftersom $p - 1$ och $q - 1$ är jämna tal.

b. I detta fall kan $\gcd(e - 1, 2p')$ och $\gcd(e - 1, 2q')$ anta tre värden 1, 2 och p' respektive q' .

I det sista fallet uppstår minst $2(p' + 1)$ odöjbara meddelanden. Sannolikheten för detta är dock bara $\approx 1/p$.

Slutsats. $p - 1$ och $q - 1$ bör innehålla stora primfaktorer och $\gcd(p - 1, q - 1)$ bör vara liten.

5.6. a. För att dechiffrera måste vi lösa $x^2 + bx \equiv y \pmod{n}$.

OBSERVERA att funktionen INTE är injektiv !

Genom att substituera $z = x + b/2$ erhålls $z^2 \equiv c \pmod{n}$, där $c = y + b^2/4$.

Detta är ekvivalent med att lösa paret $z^2 \equiv c \pmod{p}$ & $z^2 \equiv c \pmod{q}$.

Eftersom $p \equiv q \equiv 3 \pmod{4}$ är $z = \pm c^{(p+1)/4} \pmod{p}$ respektive $z = \pm c^{(q+1)/4} \pmod{q}$.

Dessa kan kombineras med CRT till fyra kvadratrötter modulo n .

Formellt kan skrivas att

$$d_K(y) = \text{sqr}[y + b^2 / 4] - b / 2 \pmod{n}.$$

b. Nu gäller att $y = x^2 + 9x \pmod{77}$ och $x = d_K(y) = \text{sqr}[y + 1] - 43 \pmod{77}$.

Med $y = 22$ behövs kvadratrötterna till 23 modulo både 7 och 11.

$$\begin{aligned} \pm 23^{(7+1)/4} &\equiv \pm 4 \pmod{7} \\ \pm 23^{(11+1)/4} &\equiv \pm 1 \pmod{11} \end{aligned}$$

Detta ger $x = 44, 24, 66$ och 2 , som alla chiffreras till 22.

5.7. Här är $x^2 \equiv y^2 \equiv a \pmod{p q}$, dvs $(x + y) * (x - y) = k p q = k n$.

Men $x \neq y$ och $x \neq n - y$ säger att $\text{gcd}(x + y, n) = p$ eller q .

5.8. a. Klartext- och chiffermängden blir så liten att det är triviale att generera tabellen

$$\langle m, m^e \pmod{n} \rangle = \langle m, c \rangle$$

för alla $m \in \{a, b, \dots, z\} = \{0, 1, \dots, 25\}$. Därefter är det bara att "läsa av" de m som motsvarar de givna c .

b. I detta exempel erhålls via $m \rightarrow m^{25} \pmod{18721}$ för $m = 0, 1, \dots, 25$ följande tabell.

Klartexten är alltså VANILLA.

a = 0	0	n = 13	4845
b = 1	1	o = 14	1375
c = 2	6400	p = 15	13444
d = 3	18718	q = 16	4540
e = 4	17173	r = 17	13663
f = 5	1759	s = 18	1437
g = 6	18242	t = 19	2940
h = 7	12359	u = 20	14858
i = 8	14930	v = 21	365
j = 9	9	w = 22	10789
k = 10	6279	x = 23	8945
l = 11	2608	y = 24	11373
m = 12	4644	z = 25	5116

5.9. $e_K(x y) \pmod{n} = (x y)^e \pmod{n} = x^e y^e \pmod{n} = x^e \pmod{n} y^e \pmod{n} = e_K(x) e_K(y) \pmod{n}$.

5.10. Notera att $\gcd(a, 561) = 1$ medför att $\gcd(a, 3) = \gcd(a, 11) = \gcd(a, 17) = 1$.

Fermats lilla sats säger oss därför att, för alla $a \in \mathbb{Z}_{561}^*$:

$$\begin{aligned} a^{560} &\equiv (a^2)^{280} \equiv 1^{280} \equiv 1 \pmod{3}. \\ a^{560} &\equiv (a^{10})^{56} \equiv 1^{56} \equiv 1 \pmod{11}. \\ a^{560} &\equiv (a^{16})^{35} \equiv 1^{35} \equiv 1 \pmod{17}. \end{aligned}$$

Enligt CRT gäller då att $a^{560} \equiv 1 \pmod{3 * 11 * 17}$, vsb.

5.11. Givet är $p = 20$ och $a = 7$. (Då blir $a^{-1} = 3$.)

a. $\mathbf{s} = \langle 1, 3, 5, 1 \rangle$ som är superökande transformeras till $\mathbf{t} = \mathbf{as} = \langle 7, 1, 15, 10 \rangle$.

b. Klartexten $\mathbf{m} = \langle 1, 1, 0, 1 \rangle$ ger $\mathbf{c} = \mathbf{t m} = 7 + 1 + 0 + 10 = 18 = \langle 1, 0, 0, 1, 0 \rangle$.

c. Dechiffreringen kan skrivas $\text{snap}(3 * 18 \bmod 20, \mathbf{s}) = 13 = \langle 1, 1, 0, 1 \rangle$.

5.12. I detta fall har vi $\alpha^{ak} = \mathbf{A}(p, a, \alpha^k, \alpha^a)$.

Nu är $p = 73$ och $\alpha = 5$ och $\alpha^k = 18$, så enligt förutsättningarna gäller att $\mathbf{A}(73, 5, 18, 49) = 8$. Klartexten x erhålls som lösningen till $x \alpha^{ak} = 7 \bmod 73$, dvs

$$8x = 7 \bmod 73, \text{ dvs } x = 10.$$

5.13.

<u>Kända relationer är</u>	<u>Många tror att</u>
RSAP \leq FACTP	RSAP \equiv FACTP
QRP \leq FACTP	QRP \equiv FACTP
SQRP \equiv FACTP	
DHP \leq DLP (i specialfall \equiv)	

Mellan RSAP och QRP vet man inget. SSP är helt oberoende av de övriga. För en "praktiker" är idag FACTP och DLP lika komplexa.

Kapitel 6

6.1. Please, uppfatta finessen i följande uträkningar. Den har med exponenterna att göra.

$$\alpha^{15} \beta^{13} \equiv \alpha^2 \beta^8 \pmod{17} \Leftrightarrow \alpha \beta^8 \alpha^{15} \beta^{13} \equiv \alpha \beta^8 \alpha^2 \beta^8 \pmod{17} \Leftrightarrow \beta^5 \equiv \alpha^3 \pmod{17}.$$

Eftersom $5^{-1} \equiv 13 \pmod{16}$ så är $(\beta^5)^{13} \equiv (\alpha^3)^{13} \pmod{17}$. Alltså $\beta \equiv \alpha^{39} \equiv \alpha^7 \pmod{17}$, dvs $\log_{\alpha} \beta = 7$. (Jämför 7.1.iv.)

6.2. $\log_2 6 \pmod{13}$ ska beräknas. Definiera tabellen enligt Shanks algoritm.

Vi finner att $m = \text{ceiling}(\text{sqrt}(13-1)) = 4$. Vi behöver α^{-1} . Ekvationen $2x \bmod 13 = 1$ ger oss $x = \alpha^{-1} = 7$. Vi ska nu iterera med $i, j \in [0, 3]$ enligt följande tabell.

j	$\alpha^{mj} \bmod p = 2^{4j} \bmod 13$	i	$\beta(\alpha^{-1})^i \bmod p = 6 \cdot 7^i \bmod 13$
0	1	0	6
1	<u>3</u>	1	<u>3</u>
2	12	2	8
3	1	3	

Då "funktionsvärdena" är lika (3) erhålls de i och j som behövs för att beräkna

$$a = \log_{\alpha} \beta = mj + i \pmod{p} = 4 \cdot 1 + 1 \pmod{13} = 5.$$

En snabbkontroll visar att detta är korrekt: $\alpha^a \equiv 2^5 \equiv 32 \equiv 6 \equiv \beta \pmod{13}$.

6.3. Förutsättningarna ger att

$$\beta\gamma^{\delta_1} \equiv \alpha^{x_1} \pmod{p}$$

$$\beta\gamma^{\delta_2} \equiv \alpha^{x_2} \pmod{p}$$

Alltså är $\alpha^{x_1 - x_2} \equiv \beta^{\delta_1 - \delta_2} \pmod{p}$.

Men $\gamma \equiv \alpha^k \pmod{p}$ och alltså

$$\alpha^{x_1 - x_2} \equiv \alpha^{k(\delta_1 - \delta_2)} \pmod{p}.$$

Då gäller att $x_1 - x_2 \equiv k(\delta_1 - \delta_2) \pmod{p-1}$, (*)

eftersom α är ett primitivt element.

Nu var emellertid $\gcd(\delta_1 - \delta_2, p - 1) = 1$ och då är (*) entydigt lösbar m a p k och när k är känd kan α beräknas ur δ -ekvationen.

6.4. Signaturen är paret $\langle \gamma, \delta \rangle$, där

$$\gamma = (\alpha^k \bmod p) \bmod q = 52^8 \pmod{103} \pmod{19} = 11.$$

$$\delta = (x + a\gamma) k^{-1} \bmod q = (12 + 19 \cdot 11) \cdot 12 \pmod{19} = 11.$$

Notera att $kk^{-1} \bmod q = 1$, dvs $8k^{-1} \bmod 19 = 1$ ger $k^{-1} = 12$.

6.5. Se avsnitt 6.4.2 i texten.

6.6. Inget svar ännu.

6.7. Utgå från $\beta = \alpha^a$, dvs $a = \log_{\alpha} \beta$ och α är ett primitivt element.

Eulers kriterium säger att $\beta^{(p-1)/2} \equiv 1 \pmod{p}$ precis då β är en kvadratisk residu.

Om α är ett primitivt element och a är jämnt så gäller $\alpha^a \in \text{QR}(p)$.

Alltså kan vi beräkna $b_1(\beta)$ genom att testa huruvida $\beta^{(p-1)/2} \equiv 1 \pmod{p}$.

6.8. ???

6.9. a. $y^x \equiv \alpha^{zx} \equiv \alpha^a \equiv \beta \pmod{p}$

b. Den publika nyckeln β och det valda meddelandet x är kända. För att bilda signaturen y är det bara att sätta $y = \beta^{x^{-1}} \pmod{p}$, där $x^{-1} x \equiv 1 \pmod{p-1}$.

Kapitel 7

7.1. Fullständighet: Antag A är ärlig. Om $i = 0$ så är $z = v^2 \pmod{n} \in \text{QR}(n)$ och $j = 0$. Om $i = 1$ så är $z = xv^2 \pmod{n}$, så $z \in \text{QNR}(n)$ och $j = 1$. B måste alltså acceptera.

Sundhet: Antag att x inte tillhör $\text{QNR}(n)$. Om $i = 1$ så är $z = xv^2 \pmod{n}$, vilket är en kvadrat. Då är $j = 0$ och B accepterar inte. Alltså: $\text{pr}[\text{B accepterar}] \leq 1/2$.

Icke ZK: B vill veta om a , säg, tillhör $\text{QR}(n)$. B kan skicka $z = a$ till A i steg 2 för att finna sanningen om a .

7.2. En kollision $\langle a1, a2 \rangle \neq \langle b1, b2 \rangle$ erhålls med godtyckligt $a1$ och $a2 = \text{RSA}(a1) \text{ xor } \text{RSA}(b1) \text{ xor } b2$, ty

7.3. Se "Korta svar till typ-tentan" (uppgift 4); appendix B.

7.4. a. Multiplikativa gruppen Z_n^* är isomorf med $Z_p^* \times Z_q^*$ så den maximala ordningen något element i Z_n^* kan ha är $\text{lcm}(p-1, q-1) = 2 p_1 q_1$.

b. Svår. Vi hoppas över denna övning.

7.5. Kirke har 50% chans att övertyga Odysseus att hon kan öppna den hemliga dörren om hon inte kan det. Upprepa proceduren så många gånger som behövs för att övertyga O. Det är alltså sunt och fullständigt. ZK-egenskapen är uppfylld ty K ger inte O någon information om låset till den hemliga dörren.

7.6. Återutsändaren upprätthåller en privat fil som korrelerar en [slump]pseudonym för avsändaren med dess verkliga identitet.

7.7. Givet ett x är det bara att ta $-x = n - x$ för att erhålla samma h .

Kapitel 8

8.1. I protokollet kan en förcör C ändra meddelandet till B till $\langle C, B, e_B(m) \rangle$.

B ser ingenting misstänkt och skickar därför tillbaka $\langle B, C, e_C(m) \rangle$ till C!

Genom att i stället använda chiffren $e_B(m, A)$ respektive $e_A(m, B)$ blir C "stoppad".

Redundans är ibland bra att ha!

8.2. Polynomet $h(x) = (2x^2 + 10x + 13) \text{ mod } 17$ ger

a. Den gemensamma nyckeln $h(0) = 13$.

b. Följande skuggor erhålls.

$$h(1) = 2 + 10 + 13 = 8.$$

$$h(3) = 18 + 30 + 13 = 61 = 10.$$

$$h(5) = 50 + 50 + 13 = 113 = 11.$$

c. Med ansatsen $ax^2 + bx + c$ erhålls ekvationssystemet (alla ekvationer modulo 17).

$$a + b + c = 8 \quad (1)$$

$$9a + 3b + c = 10 \quad (2)$$

$$25a + 5b + c = 11 \quad (3)$$

8.3. - Gemensam modulus p och generator α .

- Användare A, B, C, ... har privata "nycklar"/exponenter a, b, c, \dots

- Gemensamma nyckeln blir $K = \alpha^{abc} \dots \text{ mod } p$.

N användare måste skicka sin nyckel till $N - 1$ användare; alltså totalt $N * (N - 1)$ för att alla ska erhålla K .

8.4. Redan visat i texten.

8.5. Bloms metod ger med givna förutsättningar följande.

Förutsättningar är att $a = 23, b = 4, c = 13$ och $p = 79$.

a. $g_A(x) = a_A + b_A x = (a + br_A) + (b + cr_A)x = (23 + 4 * 1) + (4 + 13 * 1)x = 27 + 17x$.

$g_D(x) = \dots$ analogt $\dots = (23 + 4 * 2) + (4 + 13 * 4)x = 31 + 45x$.

b. $K_{A,D} = a + b(r_A + r_D) + cr_A r_D = 23 + 4*(1 + 4) + 13 * 1 * 4 = 16$.

8.6. Lösningen finns i ledningen (nästan).

8.7. t deltagare kan bestämma $k = \sum k_i$, men färre kan det inte. Notera att m inte behöver vara ett primtal och att det inte heller behöver gälla att $m \geq t + 1$, men att $w = t$.

8.8. Om tillräckligt många (hur många ?) avslöjar sin privata nyckel så kan G beräknas.

8.9. a. $K = \alpha^{bx + ay} \text{ mod } p = (\alpha^y)^a z_B^x \text{ mod } p = (\alpha^x)^b z_A^y$.

b. $K = \alpha^{x+y}$.

8.10. Detta bör väl vara trivialt i detta läge (?): $s' \text{ xor } m = k$.

Kapitel 9

9.1. "Unix-'salt' används därför att det avsevärt försvårar att gissa lösenord och försöka finna matchning med krypterade varianter avseende hela lösenordsfilen. Det försvårar inte att via 'brute force' gissa sig till en *enskild* användares lösenord, eftersom inga 'salts' är skyddade.

9.2. Redan visat i texten.

9.3. Uppenbart, eller hur ?

9.4. FFS-signatur finns redan i texten. För GQ erhålls signaturen

$$\begin{array}{ll} \gamma = k^b \bmod n & \text{Verifiering} \\ \delta = ku^{h(x, \gamma)} \bmod n & \gamma = v^{h(x, \gamma)} \delta^b \bmod n \end{array}$$

9.5. Se ledningar direkt i texten.

9.6. Inget svar.

9.7. En imitator som ser $y_i = k + ar_i$, $i = 1, 2$ kan lösa ut $a = (y_1 - y_2) (r_1 - r_2)^{-1}$.

9.8. En kvadratrot är i detta fall lätt att beräkna om faktoriseringen är känd, men givet x , y och n blir faktoriseringen enkel i 50% av fallen (se tex avsnitt 4.4.1).

9.9. a. Verifieringen blir $\gamma = \alpha_1^{y_1} \alpha_2^{y_2} v^r \pmod{p}$. b. Ganska enkelt.

Kapitel 10

10.1. I det andra fallet (högerskift) uppstår två delfall

- a. vi rör oss inom befintlig remsa.
- b. remsan måste utökas åt höger.

Kommandona blir i respektive fall.

```
a. command Cqx(s, s')
   if own ∈ A[s, s'] and q, x ∈ A[s, s] then
   delete q, x from A[s, s]
   enter Y into A[s, s]
   enter p into A[s', s']
```

b. **command** $C_{qx}(s, s')$
if end, $q, X \in A[s, s]$ **then**
delete q, X **from** $A[s, s]$
create subject s'
enter p, B **into** $A[s', s']$
enter Y **into** $A[s, s]$
delete end **from** $A[s, s]$
enter end **into** $A[s', s']$
enter own **into** $A[s, s']$

10.2 Se svar till uppgift 7 på "typtentan" i Appendix A.

10.3. Inget svar här.

10.4 Inget svar ännu.

10.5. CL effektivare, ACL lättare för administration.

10.6. a. Tag ett block b och kontrollera att $aa^{-1}(b) = b$.
 b. Ja!

Kapitel 11

11.1. För att beräkna $H(X|Y)$ behövs sannolikheterna $p(y)$ och $p(x|y)$ för alla x och y .

Med $x \in [1, 2m]$ likformigt fördelat och given **if**-sats inses att

$$p(y=0) = k/2m \qquad p(y=1) = 1 - k/2m \quad \text{-- efter det att satsen är utförd.}$$

De betingade sannolikheterna blir (efter det att satsen är genomförd)

$$\begin{array}{ll} p(x|y=0) = 1/k & \text{för } 1 \leq x \leq k \\ p(x|y=0) = 0 & \text{för övrigt} \\ p(x|y=1) = 1/(2m-k) & \text{för } k \leq x \leq 2m \\ p(x|y=1) = 0 & \text{för övrigt} \end{array}$$

Enligt definitionen av ekvokation erhålls då

$$\begin{aligned} H(X|Y) &= k/2m \sum_{[1, k]} 1/k \log k + && \{\text{för } y=0\} \\ & (2m-k)/2m \sum_{[k+1, 2m]} 1/(2m-k) \log (2m-k) = && \{\text{för } y=1\} \\ & = k/2m \log k + (2m-k)/2m \log (2m-k). \end{aligned}$$

Informationsöverföringen $I = H(X) - H(X|Y)$ maximeras därför för $k = m$.

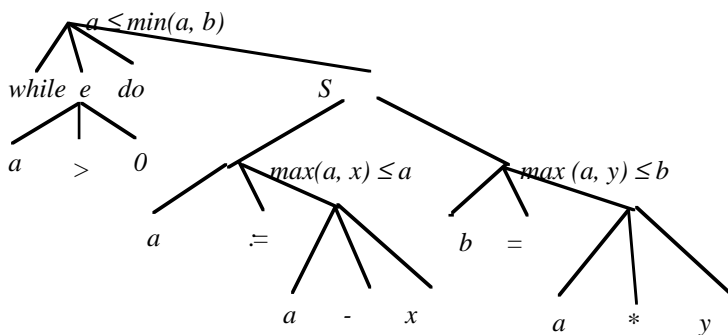
11.2. Av symmetriskäl inses att $H(X|Z') = H(Y|Z')$ så beräkna den första som är

$$- \sum_{[0,1]} p(z) \sum_{[0,1]} p(x|z) \log p(x|z).$$

Tabellen	ger	följande värden															
<table style="border-collapse: collapse; width: 100%;"> <tr> <td style="padding: 2px 10px;">x</td> <td style="padding: 2px 10px;">y</td> <td style="padding: 2px 10px;">z</td> </tr> <tr> <td style="padding: 2px 10px;">0</td> <td style="padding: 2px 10px;">0</td> <td style="padding: 2px 10px;">0</td> </tr> <tr> <td style="padding: 2px 10px;">0</td> <td style="padding: 2px 10px;">1</td> <td style="padding: 2px 10px;">0</td> </tr> <tr> <td style="padding: 2px 10px;">1</td> <td style="padding: 2px 10px;">0</td> <td style="padding: 2px 10px;">0</td> </tr> <tr> <td style="padding: 2px 10px;">1</td> <td style="padding: 2px 10px;">1</td> <td style="padding: 2px 10px;">1</td> </tr> </table>	x	y	z	0	0	0	0	1	0	1	0	0	1	1	1		$p(z = 0) = 3/4$ $p(z = 1) = 1/4$
x	y	z															
0	0	0															
0	1	0															
1	0	0															
1	1	1															
		$p(x = 0 z = 0) = 2/3$ $p(x = 0 z = 1) = 0$ $p(x = 1 z = 0) = 1/3$ $p(x = 1 z = 1) = 1$															

$$H(X | Z') = 3/4 * 2/3 * \log 3/2 + 3/4 * 1/3 * \log 3 = 3/4 * \log 3 - 1/2 \approx 0.7.$$

11.3.



Det blir alltså de tre utskrivna villkoren att kontrollera.

11.4. Med följande utgångspunkter:

Delmängdslattice S med	Total ordning T med
low = tomma mängden	$low = 0$
$high$ = hela mängden	$high$ = "något stort tal" N
partiell ordning = delmängd	partiell ordning = vanligt \leq
lub = union	lub = maximum
glb = snitt	glb = minimum

kan bildas ett lattice på $S \times T$ via

$\langle s, t \rangle \leq \langle s', t' \rangle$	\Leftrightarrow	$t \leq t' \ \& \ s$ delmängd av s'
$lub(\langle s, t \rangle, \langle s', t' \rangle)$	\Leftrightarrow	$\langle \cup(s, s'), \max(t, t') \rangle$
$glb(\langle s, t \rangle, \langle s', t' \rangle)$	\Leftrightarrow	$\langle \cap(s, s'), \min(t, t') \rangle$
$low = \langle \emptyset, 0 \rangle$		
$high = \langle S, N \rangle$		

Det är lätt att se att resultatet är ett lattice; verifiera själv att alla villkor är uppfyllda.

11.5. Här efterfrågas $I = H(X) - H(X | Y')$ för **if** $x > 0$ **then** $y := 1$; **--** $y = 0$ initialt då

$$p(x = 0) = 0.5, p(x = 1) = 0.25 = p(x = 2).$$

De givna sannolikheterna ger direkt entropin:

$$H(X) = 1/2 \log 2 + 2 * 1/4 \log 4 = 1 1/2.$$

För att bestämma $H(X | Y') = \sum_y p(y) \sum_x p(x | y) \log p(x | y)$ beräknas sannolikheterna:

$$\begin{array}{ll}
 p(y=0) = 0.5 & p(y=1) = 0.5 \\
 p(x=0 | y=0) = 1 & \\
 p(x=0 | y=1) = 0 & \\
 p(x=1 | y=0) = 0 & \\
 p(x=1 | y=1) = 0.5 & \\
 p(x=2 | y=0) = 0 & \\
 p(x=2 | y=1) = 0.5 &
 \end{array}
 \begin{array}{l}
 x \ y \\
 \hline
 0 \ 0 \\
 1 \ 1 \\
 2 \ 1
 \end{array}$$

Detta ger $H(X | Y) = 0.5 * [1 \log 1 + 0 \log 0 + 0 \log 0] + 0.5 * [0 \log 0 + 1/2 \log 2 + 1/2 \log 2] = 1/2$

Alltså $I = 1/2$

11.6. En **case** (switch)-sats:

case a **of** $v_1: S_1; \dots v_n: S_n; \mathbf{end\ case};$

kan "översättas" till en **if**-sats:

if a = v_1 **then** S_1
 else if a = v_2 **then** S_2
 ...
 else if a = v_n **then** $S_n;$

Enligt certifiering av **if**-sats, upprepad n gånger, erhålls följande uttryck.

$$(a \oplus) \oplus_{i \in [1, n]} \forall i \leq \otimes_{i \in [1, n]} X_i,$$

där $X_i = \{\text{objekt som tilldelas värden i } S_i, \dots, S_n\}$.

Vidare krävs att alla S_i är flödessäkra i sig. (Beteckningen $\underline{x} = c(x)$ har använts.)

11.7. a. Satsen **if** a = b **then** $c := a;$ kräver att $\underline{a} \oplus \underline{b} \leq \underline{c}$ och att $\underline{a} \leq \underline{c}$.

Enligt förutsättningarna är detta inte uppfyllt: $\underline{b} \leq \underline{c}$. Satsen är alltså inte tillåten.

b. Satsen **begin** $b := a; d := b, c := d; \mathbf{end};$ är inte tillåten pga att inte $\underline{d} \leq \underline{c}$.

c. Satsen $c := a + b + c + d;$ kräver att "alla" är $\leq \underline{c}$. Så är inte fallet. Inte tillåten.

11.8. a. Frågan är densamma som 11.2.

b. Följande villkor är nödvändiga för flödessäkerhet.

$$\underline{x} \oplus \underline{y} \leq \underline{z} \quad \text{och} \quad \underline{1} \leq \underline{z} \quad (\text{Detta är trivialt uppfyllt eftersom } \underline{1} = \text{low}.)$$

11.9. Ledning. Notera att $x^{p-1} \bmod p$ (enligt Fermat) är 1 för $x = 1, 2, \dots, p-1$ och lika med 0 för $x = p$.

Kapitel 12

12.1. Några karakteristika är följande:

Kryptering på transportnivå

Vanligen programvara
Ingen klartext i noderna
EN kryptonyckel
Start- och slutadresserna i klartext i nätet
Applikationen chiffrerar

Kryptering på datalänknivå

Vanligen maskinvara
Klartext i noderna
Varje nod-par har egen nyckel
Dessa kan krypteras i nätet
Chiffrering görs i underliggande skikt

Fyll (gärna) själv i flera.

12.2. Det är svårt att konvertera till ett B3-system eftersom det behövs en verifierbar kärna. Ett B3-system måste i praktiken byggas som ett sådant från grunden.

12.3.

Vi har att $D(p \parallel q) = -\sum_x p(x) \log [q(x) / p(x)] \geq \{\text{enligt it-olikheten}\} \geq$

$-\log e \sum_x p(x) [q(x) / p(x) - 1] = -\log e [\sum_x q(x) - \sum_x p(x)] = -\log e [1 - 1] = 0.$

12.4. Det gäller att $a = 121^n + 5 \cdot 25^n - 6.$

Första termen ger rest 1 vid division med 24. Andra termen ger rest 5 vid division med 24. Tredje termen ger rest -6 vid division med 24. Alltså: $a \equiv 0 \pmod{24}.$

12.5. Ekvationen i texten är ekvivalent med $C_k f = f C_k.$

Denna kan också skrivas $C_k f(a) = f C_k(a)$ eller $f(a) + k = f(a + k).$

Om $a = 0$ erhålls $f(k) = f(0) + k$ vilket säger att $f = C_{f(0)}$ är en lösning.

12.6. Inget svar ännu.

12.7. Inget svar ännu. Satsen behövs för att kunna dechiffrera.

12.8. Sense moral: Signera inte "vad som helst"!

Vad innebär följande sekvens (D. Knuths sätt att byta innehållet i två variabler "utan att använda någon temporär variabel")?:

```
a := a xor b
b := a xor b
a := a xor b
```

Andra satsen ger, efter att den första utförts, ju att $a \rightarrow b$. Tredje satsen ger sedan att $b \rightarrow a$.

Så långt är allt väl, men den gode Knuth luras när han påstår att temporär inte behövs!
Man ser den inte i denna "högnivåbeskrivning". ALU-n har ett resultatregister!

Här kommer sista övningen:

Chain Reaction -- Timing: 12

From any quarter tag or quarter line formation in which each very centers can Pass Thru with an outside dancer.

[At Advanced, this call is restricted to starting from right- or left-hand quarter tag formations only.]:

The very centers PassThru with the dancers they are facing, while the ends of the center line/wave Promenade 1/4 around the outside of the set.

The original very centers and the dancers they are next to, Hinge.

The centers star (or Diamond Circulate) one spot, while the outsides Trade.

Those who meet now Cast Off 3/4, while the others move up (as in Hourglass Circulate) to become the ends of parallel waves.

