Matematiska Institutionen
KTH

Lösningar till några övningar på felkorrigerande koder, RSA-kryptering och permutationer inför lappskrivning 6 media.

1. Betrakat ett RSA-krypto med $n = 51$ och $e = 5$. Kryptera meddelandet 3 och dekryptera meddelandet 5.

   Lösn. Allmänt gäller att det krypterade meddelandet blir $E(a) = a^e \pmod{n}$. Vi får alltså

   $$E(3) \equiv_{51} 3^5 \equiv_{51} 3^4 \cdot 3 \equiv_{51} 30 \cdot 3 \equiv_{51} 90 \equiv_{51} 29.$$

   Dekrypteringsnyckeln är $D(b) = b^d \pmod{n}$ där, om $n = pq$ så $m = (p-1)(q-1)$ och $e \cdot d \equiv 1 \pmod{m}$. Vi får $p = 3$ och $q = 17$ så $m = 2 \cdot 16 = 32$. För att finna d använder vi nu Euklides algoritm i sökandet efter $sgd(5, 32)$:

   $$\begin{array}{l} 32 = 6 \cdot 5 + 2 \\ 5 = 2 \cdot 2 + 1 \end{array} \quad \text{varur} \quad \left[\begin{array}{l} 1 = 5 - 2 \cdot 2 = 5 - 2(32 - 6 \cdot 5) = \\ 13 \cdot 5 - 2 \cdot 32. \end{array} \right] \quad \text{dvs} \quad 1 \equiv_{32} 13 \cdot 5.$$

   Sålunda $d = 13$ och $D(5) = 5^13 \equiv_{51} 5^8 \cdot 5^4 \cdot 5$. Vi finner att

   $$5^4 \equiv_{51} 5^2 \cdot 5^2 \equiv_{51} 625 \equiv_{51} 12 \cdot 51 + 13 \equiv_{51} 13$$

   och

   $$5^8 \equiv_{51} 5^4 \cdot 5^4 \equiv_{51} 13 \cdot 13 \equiv_{51} 169 \equiv_{51} 16.$$

   Alltså

   $$D(5) \equiv_{51} 16 \cdot 13 \cdot 5 \equiv_{51} 16 \cdot 65 \equiv_{51} 16 \cdot 14 \equiv_{51} 20.$$

2. Betrakta ett RSA-krypto med $n = 57$. Du får välja parametern e själv. Skriv upp de möjliga val av parametern e du har.

   Lösn. Precis de tal e sådana att $sgd(e, m) = 1$, där $n = pq$ och $m = (p-1)(q-1)$ duger. Vi har $p = 3$ och $q = 19$ så $m = 36$. Alla tal e mellan 1 och 35 sådana att inget av talen 2 eller 3 delar e duger. Detta ger vårt svar.

3. Visa med hjälp av ett lämpligt Fermattest att talet 18 inte är ett primtal.

   Lösn. Om $b^{p-1} \not\equiv 1 \pmod{p}$ för något tal b så är p inte ett primtal, för som man säger, talet p klarade inte i så fall Fermattestet med bas b.

   Vi kollar med $b = 2$. Då $2^4 \equiv_{18} (-2)$ så

   $$2^{16} \equiv_{18} (2^4)^4 \equiv_{18} (-2)^4 \equiv_{18} 2^4 \equiv_{18} -2,$$

   så får vi

   $$2^17 \equiv_{18} 2^{16} \cdot 2 \equiv_{18} -2 \cdot 2 \equiv_{18} -4 \not\equiv_{18} 1.$$

4. Låt C vara en 1-felsrättande kod med kontrollmatrisen

$$H = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 \end{bmatrix}.$$

a) Bestäm antalet ord i koden C.

Lösn. Kolonnerna 1, 2, 5, 6 och 7 är linjärt beroende så matrisens rang blir 5. Då totala antalet kolonner är 8 blir antalet ord $2^{8-5} = 8$.

b) Bestäm minst fem olika ord i C.

Lösn. Ordet $\bar{x} = (x_1, x_2, \ldots, x_8)$ tillhör koden precis då

$$H\bar{x}^T = \bar{0}.$$

Vi löser detta linjära ekvationssysytem på sedvanligt sätt och får lösningsmängden

$$\bar{x} = (x_1, x_2, \ldots, x_8) = t(1,0,1,1,1,1,1,1) + s(0,0,0,1,0,0,1,1) + u(0,1,1,1,1,0,0,0).$$

Observera att det finns flera andra sätt att beskriva lösningsmängden Vi väljer nu t ex $(t, s, u) \in \{(0,0,0), (1,0,0), (0,1,0), (0,0,1), (1,1,0)\}$ och får då orden 00000000, 10111111, 00010011, 01111000, 10101100.

c) Ordet 11111111 ligger på avståndet ett från precis ett ord i C. Vilket.

Lösn. $H(1,1,1,1,1,1,1,1)^T = (0,1,0,1,1)^T$ vilket är den andra kolonnen i matrisn H. Alltså var felet i poistion 2 och det sökta ordet var 10111111.

d) Bestäm minst ett ord av längd åtta som inte tillhör C och som inte ligger på avståndet ett från något kodord.

Lösn. Vi chansar och tar ett ord på måfå 11100000. Vi finner att

$$H \begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 1 \\ 1 \end{bmatrix}$$

vilket ju inte ár någon av H:s kolonner. Alltså ligger ordet på ett avstånd större än ett från alla kodord.

e) Bestäm antalet binära ord av längd åtta som varken tillhör C eller ligger på avståndet ett från något ord i C.

Lösn. Varje sfär med radien 1 runt något kodord innehåller $1 + 8$ stycken ord. Då koden är 1-felsrättande så är sfärerna med radien ett runt kodorden disjunkta. Totalt finns 8 kodord så antalet ord på avstånd ett från något kodord blir då $8 \cdot (1 + 8)$ Totalt finns 2^8 stycken ord. De ord som inte ligger i någon 1-sfär går inte att rätta.

5. Låt $\varphi = (1\ 2\ 4\ 7)(3\ 5\ 6)$, $\psi = (1\ 5\ 3)(4\ 2)(6\ 7)$ och $\gamma = (1\ 2\ 3\ 4\ 5\ 6\ 7)$.

   a) Skriv permutationerna $\varphi\psi\gamma$ och $\psi\gamma\varphi$ som produkter av disjunkta cykler.

   b) Bestäm $\psi^{-1}\varphi^{-1}$.

   Lösn. För att få inverserna av permutationerna vänder vi bara på ordningen i cyklerna. Vi får $\varphi^{-1} = (7\ 4\ 2\ 1)(6\ 5\ 3)$ och $\psi{-}1 = (3\ 5\ 1)(2\ 4)(7\ 6)$.

   c) Beräkna $\psi^{-1}\gamma\psi$.

   d) Bestäm ordningen hos permutationerna $\psi^{-1}\varphi^{-1}$, γ och $\psi^{-1}\gamma\psi$.

   Lösn. Vi använder att ordningen av en cykel är lika med cykellängden samt att om cyklerna är disjunkta, dvs saknar gemensamma element, så är ordningen av produkten av dessa cykler lika med den minsta gemensamma multipeln av alla cykellängder.

   e) Skriv permutationerna φ, ψ och γ som produkter av transpositioner.

   Lösn. Det finns många sätt att skriva en cykel som en produkt av transpositioner. Ett sätt är följande:

   $$(a_1\ a_2\ a_3\ a_4\ \ldots\ a_{n-1}\ a_n) = (a_1\ a_n)(a_1\ a_{n-1})(a_1\ a_{n-2})\ldots(a_1\ a_4)(a_1\ a_3)(a_1\ a_2).$$

   Använder vi denna metod så får vi svaret.

   f) Vilka av permutationerna i uppgift d) är udda respektive jämna.

   Lösn. En permutation är jämn om den kan skrivas som en produkt av ett jämnt antal permutationer annars är den udda. Använder vi dett får vi svaret.

Svar:

1. $E(3) = 39$, $d = 13$ ger att $D(5) = 20$.
2. 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35.
3.
4. a) 16, b) , c) 10111111, d) 11100000, e) $2^8 - 16 \cdot (1 + 8)$.
5. a) $\varphi\psi\gamma = (1\ 7\ 6\ 3\ 4\ 5)(2)$ och $\psi\gamma\varphi = (1)(2\ 3\ 7\ 4\ 5\ 6)$.
   b) (1 6)(2 3 7)(4)(5)
   c) (1 7 6 3 4 5 2)
   d) 6, 7 resp 7.
   e) $\varphi = (1\ 7)(1\ 4)(1\ 2)$, $\psi = (1\ 3)(1\ 5)(4\ 2)(6\ 7)$, $\gamma = (1\ 7)(1\ 6)(1\ 5)(1\ 4)(1\ 3)(1\ 2)$.
   f) φ är udda och de övriga är jämna.