Uppgift 3: Problemlösningsuppgift – Kryptografi

Fråga 3.1. I en viss enkel form av kryptografi ersätts varje bokstav med ett motsvarande tal (A = 1, B = 2, osv). Vi använder det vanliga svenska alfabetet med 29 bokstäver i den här uppgiften: 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, Å, Ä, Ö. (Sammanlagt 7 p.)

(a) Namnet på en ort i Finland har krypterats med det enkla kryptogrammet som beskrivs ovan, vilket ger oss följande krypterade meddelande:
11 15 18 19 8 15 12 13
Dekryptera meddelandet. Vad är det krypterade ordet? (1 p.)

(b) Här har samma meddelande skrivits, men med en mera invecklad kryptering. Där har startplatsen för talen flyttats ett visst antal steg framåt, så att t.ex. D = 1, E = 2, osv, och efter den sista bokstaven fortsätter det till början av alfabetet så att varje bokstav får ett motsvarande krypteringstal. Nu är det krypterade meddelandet följande:
9 13 16 17 6 13 10 11.
Hur mycket har startplatsen för talen flyttats framåt? (1 p.)

(c) Anta att du inte vet vilket ord som finns i fråga 3.1.(b), du vet att krypteringen baserar sig på just denna metod, men vet inte hur många steg bokstäverna har flyttats. Ge exakta instruktioner för dekrypteringen. Gör instruktionerna så klara och exakta att vilken som helst ungdom i gymnasieåldern skulle kunna följa dem. (5 p. Betygsättningen tar i beaktande hur tydlig, konsekvent och fungerande lösningen är.)

Fråga 3.2. I en annan kryptering har bokstäverna ersatts med andra bokstäver som är i motsatt ordning (A = Ö, B = Ä, osv). (Sammanlagt 10 p.)

(a) Dekryptera följande meddelande, som innehåller namnet på en ort i Finland: PBLNYK (1 p.)

(b) Följande meddelande har krypterats med en mera invecklad version av krypteringen. Där har bokstäverna flyttats som i fråga 3.1.(b), så J är inte T i krypteringen, utan W med ett visst antal flytt. Dekryptera följande meddelande, som innehåller namnet på en ort i Finland: MVKRÄÅE. Du vet alltså inte hur många steg bokstäverna har flyttats, utan du måste ta reda på det. (3 p.)

(c) Anta att du inte vet vilket ord som finns i fråga 3.2.(b), du vet att krypteringen baserar sig på just denna metod, men vet inte hur många steg bokstäverna har flyttats. Ge exakta instruktioner för dekrypteringen. Gör instruktionerna så klara och exakta att vilken som helst ungdom i gymnasieåldern skulle kunna följa dem. (5 p. Betygsättningen tar i beaktande hur tydlig, konsekvent och fungerande lösningen är.)

(d) Hur många flyttalternativ måste du högst testa för att kunna utföra dekrypteringen? (1 p.)

Fråga 3.3. Låt oss sedan se på s.k. asymmetrisk kryptering, där nyckeln för krypteringen är öppen dvs offentlig för alla, medan endast mottagaren av meddelandet vet nyckeln för dekryptering. Den här metoden används allmänt till att kryptera meddelanden nuförtiden. Med krypteringsmetoden krypterar man tal, vilket innebär att bokstäver och övriga tecken förvandlas till tal först och sedan krypteras.

Asymmetrisk kryptering fungerar så här: Först väljer man två primtal p och q. Med primtal avses naturliga tal > 1 som endast är delbara med 1, men inte med något annat tal som är mindre än talet självt. Primtal är alltså 2, 3, 5, 7, 11, 13, 17, 19, osv.

Räkna talens produkt $p * q = N$. Välj sedan ett tal d så att $1 < d < N$, och så att talen d, $(p-1)$ och $(q-1)$ inte har gemensamma nämnare. Talen har en gemensam nämnare om de är delbara med samma tal.

Välj sedan talet x så att om man delar $d * x$ med talet $(p-1) * (q-1)$ så får man resten 1.

Nu har vi fått reda på de öppna krypteringsnycklarna N och x, och dekrypteringsnycklarna N och d. Nycklarna N och x kan publiceras fast på webben, men nyckeln d måste hållas hemlig så att ingen obehörig kan dekryptera meddelandet.

Låt oss betrakta detta via ett exempel. Välj $p = 3$ och $q = 11$, vilket ger $N = p * q = 33$ och $(p-1) * (q-1) = 20$. Nu måste det vara så att $1 < d < 33$, och d får inte ha någon gemensam nämnare med talen 2 och 10. Ett sådant värde på d är exempelvis 3. Nu måste vi välja x så att resten då $3 * x$ divideras med 20 är 1. Vi kan välja $x = 7$.

Det öppna nyckelparet är alltså $N = 33$ och $x = 7$. Det hemliga nyckelparet är $N = 33$ och $d = 3$.

Meddelandet krypteras så att det upphöjs i x:te potens och sedan tas resten av en division med N. Det krypterade meddelandet dekrypteras så att det upphöjs i d:te potens och sedan tas resten av en division med N. (Sammanlagt 8 p.)

(a) Kari vill skicka Taina ett meddelande om vilken tågvagn de ska träffas i. Kryptera meddelandet 2 med den asymmetriska krypteringsmetoden beskriven ovan. (3 p.)

(b) Taina svarar med ett meddelande om vilket klockslag, med en timmes noggrannhet, de ska träffas. Det krypterade meddelandet är 6. Dekryptera meddelandet och ta reda på mötestiden. (5 p.)