Övningar till kapitel 6: Introduktion till Kryptering och RSA

6.2. Caesars krypto

6.2.1. Utgående från att A, E och R är mycket vanliga bokstäver i det svenska språket, dekryptera följande text:

"ZQW AQD AHOFJUHQ ESX TUAHOFJUHQ COSAUJ RHQ"

OBS: Bokstäverna Å, Ä och Ö har utelämnats och dessa är en Caesarrullning baserat på det engelska alfabetet: ABCDEFGHIJKLMNOPQRSTUVWXYZ. Meningen är dock svensk. Bokstavskombinationen ERA är mycket vanlig i svenskan.

6.2.2. Kryptera följande text med Vigenèrekryptot: ”DETTA BLIR JÄTTESVÅRT ATT LÄSA”, med rullningsstegen 2, 5, 1.

6.2.3. Förklara varför ett engångskrypto är fullständigt säkert.

6.3. Nycklar

6.3.1. Redogör för nyckeldistributionsproblemet.

6.3.2. Ange nyckeln till kryptot i 6.2.1.

6.3.3. Låt följande RSA-instans vara given:

$$encrypt(T) = T^3 (mod 22) \qquad decrypt(C) = C^7 (mod 22)$$

Fullborda nedanstående tabeller:

T	$encrypt(T) = T^3 (mod 22)$
0	0
1	
2	
3	5
4	
5	15
6	
7	13
8	6
9	
10	10
11	11
12	12
13	19
14	
15	9
16	4
17	
18	

T	$encrypt(T) = T^3 (mod 22)$
19	17
20	
21	21

C	$decrypt(C) = C^7 (mod 22)$
0	0
1	1
2	18
3	
4	16
5	3
6	
7	
8	2
9	
10	10
11	11
12	12
13	
14	
15	5
16	14
17	
18	
19	
20	4
21	21

6.4. Assymmetriska krypton och RSA-kryptot

6.4.1. Förklara betydelsen av assymmetriskt och symmetriskt krypto.

6.4.2. Låt talen *a* och *b* vara givna. Med hjälp av Euklides utvidgade algoritm kan man finna tal *x* och *y* sådana att *x***a* + *y***b* = GCD(*a*, *b*). Finn *x*, *y* och GCD(*a*, *b*) för följande par av tal:

2100 och 5670 3150 och 13860 6300 och 20790

6.4.3. Verifiera att talen *p* = 83, *q* = 89, *N* = 7387, *e* = 17 och *d* = 849 uppfyller kraven som ställs i RSA-kryptot.

Blandade övningar

(Blandade övningar är för det mesta av tentamenskaraktär)

6.1. Finn två uppsättningar tal *x* och *y* samt *u* och *v* sådana att *x**154 + *y**195 = 1 och *u**154 + *v**195 = 1 där *x* är positivt och *u* är negativt.

6.2. Finn två uppsättningar tal x och y samt u och v sådana att $x*110 + y*273 = 1$ och $u*110 + v*273 = 1$ där x är positivt och u är negativt.

6.3. Finn två uppsättningar tal x och y samt u och v sådana att $x*255 + y*182 = 1$ och $u*255 + v*182 = 1$ där x är positivt och u är negativt.

6.4. Bilda en instans av RSA baserad på primtalen 47 och 59.

6.5. Bilda en instans av RSA baserad på primtalen 23 och 83. Välj e större än 3.

6.6. Bilda en instans av RSA baserad på primtalen 7 och 107.

6.7. Bilda en instans av RSA baserat på primtalen 11 och 89. Välj e större än 3.

6.8. Ett så kallat säkert primtal p är ett primtal där även $(p - 1) / 2$ är ett primtal. Vilka av instanserna av RSA i uppgifterna 6.4, 6.5, 6.6 och 6.7 ovan är baserade på säkra primtal?

6.9. Löses med Maple. En instans av RSA formeras för att kryptera 128-bitarstal (unsigned binary). För den skull måste p och q väljs så att produkten pq överstiger 2 ^ 128. Hur många bitar behövs för att lagra de krypterade talen?

Ledning: Försök välja p och q så att produkten pq blir så liten som möjligt. Hur många bitar behövs för att representera N = pq?

Facit till övningar till kapitel 6: Introduktion till Kryptering och RSA

6.2. Caesars krypto

6.2.1. Utgående från att A, E och R är mycket vanliga bokstäver i det svenska språket, dekryptera följande text:

"ZQW AQD AHOFJ**UHQ** ESX TUAHOFJ**UHQ** COSAUJ RHQ"

Vi ser att tre vanliga bokstäver i kryptotexten är U, H och Q. Bokstavskombinationen ERA är mycket vanlig i svenskan och vi ser att bokstavsföljden UHQ förekommer på två ställen. (Fetmarkerat i kryptotexten.) Vi gissar därför att att UHQ = ERA. Om detta stämmer skulle kryptotexten ha resulterat från en kryptering med Caesarrullning i 16 steg. Om vi rullar tillbaka 16 steg finner vi att klartexten: ”JAG KAN KRYPTERA OCH DEKRYPTERA MYCKET BRA”.

6.2.2. Kryptera följande text med Vigenèrekryptot: ”DETTA BLIR JÄTTESVÅRT ATT LÄSA”, med rullningsstegen 2, 5, 1.

Vi tar rullningarna var för sig, först de i två steg, det är var tredje bokstav med början på D. Sedan tar vi rullningarna i 5 steg. Det blir också var tredje bokstav men med början på E. Allra sist tar vi rullningen i ett steg. Det blir var tredje bokstav men med början på T:

”D E T T A B L I R J Ä T T E S V Å R T A T T L Ä S A” rullas i två steg till

”F E T V A B N I R L Ä T V E S X Å R V A T V L Ä U A” rullas i 5 steg till

”F J T V F B N N R L D T V J S X C R V F T V Q Ä U F” rullas i 1 steg till

”F J U V F C N N S L D U V J T X C S V F U V Q Ö U F” som ihopskrivet blir

”FJUVF CNNS LDUVJ TXCSV FUV QÖUF”. (Vilken röra!)

6.2.3. Ett engångskrypto baseras på en fullständigt slumpmässig följd av nycklar där varje nyckel krypterar ett tecken i klartexten. Eftersom denna följd är fullständigt slumpmässig är alla mönster fullständigt utplånade varför inga analyser som helst förmår extrahera det dolda innehållet.

6.3. Nycklar

6.3.1. Redogör för nyckeldistributionsproblemet.

Nyckeldistributionsproblemet uppkommer då de två aktörerna i krypteringstillämpningar, Alice och Bob, vill komma överens om vilka nycklar de ska använda för att kryptera sina meddelanden. Eftersom de inte har en säker kanal att kommunicera med finns ingen möjlighet att säkert överföra en nyckel med ett symmetriskt krypto. (Typ Caesar.) Alice och Bob måste använda ett assymmetriskt krypto eller ett engångskrypto om de vill gardera sig för tjuvlyssnarens attacker.

6.3.2. Ange nyckeln till kryptot i 6.2.1.

Nyckeln är 16 eftersom rullningen var i 16 steg.

6.3.3.

T	$encrypt(T) = T^3 (mod 22)$
0	0
1	1
2	8
3	5
4	20
5	15
6	18
7	13
8	6
9	3
10	10
11	11
12	12
13	19
14	16
15	9
16	4
17	7
18	2
19	17
20	14
21	21

C	$decrypt(C) = C^7 (mod 22)$
0	0
1	1
2	18
3	9
4	16
5	3
6	8
7	17
8	2
9	15
10	10
11	11
12	12
13	7
14	20
15	5
16	14
17	19
18	6

C	$decrypt(C) = C^7 (mod 22)$
19	13
20	4
21	21

6.4. Assymmetriska krypton och RSA-kryptot

6.4.1. Förklara betydelsen av assymmetriskt och symmetriskt krypto.

Ett symmetriskt krypto har samma nyckel som används för dekryptering som används för kryptering. Exempel: Caesar/Vigenère, DES/TripleDES, engångskrypton. Ett assymmetriskt krypto har olika nycklar för kryptering och dekryptering. Exempel: RSA.

6.4.2. *Svar:*

GCD(2100, 5670) = 210 och -8*2100 + 3*5670 = 210.

GCD(3150, 13860) = 630 och 9*3150 - 2*13860 = 630.

GCD(6300, 20790) = 630 och 10*3150 - 3*13860 = 630.

6.4.3. Verifiera att talen $p = 83$, $q = 89$, $N = 7387$, $e = 17$ och $d = 849$ uppfyller kraven som ställs i RSA-kryptot.

$(p - 1)(q - 1) = 82*88 = 2*41*2*44 = 2*41*2*2*2*11 = 2^4*11*41$. Detta tal och $e = 17$ är relativt prima. Vi ser även att $e*d = 17*849 = 14433 = 14432 + 1 = 2*82*88 + 1$ vilket innebär att 17*849 är kongruent med 1 modulo $82*88 = (p - 1)(q - 1)$. Detta är kraven som RSA ställer.

Blandade övningar

(Blandade övningar är av tentamenskaraktär)

6.1. Svar: $x = 19$ och $y = -15$ samt $u = -176$ och $v = 139$.

6.2. Svar: $x = 206$ och $y = -137$ samt $u = -67$ och $v = 27$.

6.3. Svar: $x = 5$ och $y = -7$ samt $u = -177$ och $v = 248$.

6.4. Svar: Till exempel $e = 3$, $d = 1779$ och $N = pq = 2773$.

6.5. Svar: Till exempel $e = 5$, $d = 361$ och $N = pq = 1909$.

6.6. Svar: Till exempel $e = 5$, $d = 509$ och $N = pq = 749$.

6.7. Svar: Till exempel $e = 7$, $d = 503$ och $N = pq = 979$.

6.8. Svar: Alla utom 6.7 är baserade på säkra primtal där 89 inte är ett säkert primtal. (89 – 1) / 2 = 88 / 2 = 44 som inte är ett primtal.

6.9. Om vi drar roten ur 2 ^ 128 får vi 18446744073709551616. Om vi med *Maple*-funktionen safeprime tar fram ett primtal som är större än detta får vi p = 18446744073709563863. Vi använder *Maple* en gång till för att ta fram ett primtal till större än detta och erhåller q = 18446744073709564343. Produkten av p och q blir nu pq = 340282366920938924152361104254266137009. Detta är ett tal som anger hur många olika tal vi kan kryptera med denna instans av RSA. (Vi har ännu inte valt e och d och kommer heller inte att göra det.) Poängen är att detta tal är större än 2 ^ 128 men mindre än 2 ^ 129. Det betyder att att vi måste använda *129 bitar* för att representera de krypterade 128-bitarstalen.