Kryptooppgave Løsningsforslag

Hans J. Rivertz

9. august 2019

1 Oppgavene

Oppgave 1

I denne oppgaven skal du bruke RSA med offentlig nøkkel $n = 713 = 23 \cdot 31$ og $e = 43$.

a) Kryptér meldingen KOM (oversett den først til tall, A=1, B=2, osv, og krypter hvert tall med RSA). Ta med all mellomregning.

Svar: Oversetter til tall: K=11, M=13, O=15

Skriver 43 som 32+11=32+8+3=32+8+2+1.

$$\begin{aligned} 11^2 &\equiv 121 \pmod{713} \\ 11^4 \equiv 121^2 &\equiv 381 \pmod{713} \\ 11^8 \equiv 381^2 &\equiv 422 \pmod{713} \\ 11^{16} \equiv 422^2 &\equiv 547 \pmod{713} \\ 11^{32} \equiv 547^2 &\equiv 462 \pmod{713} \end{aligned}$$

$$11^{43} = 11^{32}11^8 11^2 11 \equiv 462 \cdot 422 \cdot 121 \cdot 11 \equiv 21 \pmod{713}$$

$$\begin{aligned} 13^2 &\equiv 169 \pmod{713} \\ 13^4 \equiv 169^2 &\equiv 41 \pmod{713} \\ 13^8 \equiv 41^2 &\equiv 255 \pmod{713} \\ 13^{16} \equiv 255^2 &\equiv 142 \pmod{713} \\ 13^{32} \equiv 142^2 &\equiv 200 \pmod{713} \end{aligned}$$

$$13^{43} = 13^{32}13^8 13^2 13 \equiv 200 \cdot 255 \cdot 169 \cdot 13 \equiv 576 \pmod{713}$$

$$\begin{aligned} 15^2 &\equiv 255 \pmod{713} \\ 15^4 \equiv 255^2 &\equiv 2 \pmod{713} \\ 15^8 \equiv 2^2 &\equiv 4 \pmod{713} \\ 15^{16} \equiv 4^2 &\equiv 16 \pmod{713} \\ 15^{32} \equiv 16^2 &\equiv 32; \pmod{713} \end{aligned}$$

$$15^{43} = 15^{32}15^{8}15^{2}15 \equiv 256 \cdot 4 \cdot 255 \cdot 15 \equiv 89 \pmod{713}$$

Kodet tekst $\{21, 576, 89\}$.

b) Finn minste positive invers for 43 modulo 660.

Svar: Euklids utvidede algoritme fram

$$\begin{aligned} 660{:}43{=}15 &\text{ Rest } 15 \\ 43\ {:}15{=}\ 2 &\text{ Rest } 13 \\ 15\ {:}13{=}\ 1 &\text{ Rest }\ 2 \\ 13\ {:}\ 2 = 6 &\text{ Rest }\ 1 \\ 2\ {:}\ 1 = 1 &\text{ Rest }\ 0 \end{aligned}$$

og tilbake

$$\begin{aligned} 1 &= 13 - 6 \cdot 2 = 13 - 6(15 - 13) \\ &= 7 \cdot 13 - 6 \cdot 15 = 7 \cdot (43 - 2 \cdot 15) - 6 \cdot 15 \\ &= 7 \cdot 43 - 20 \cdot 15 = 7 \cdot 43 - 20 \cdot (660 - 15 \cdot 43) \\ &= 261 \cdot 43 - 20 \cdot 660 \end{aligned}$$

Det betyr at

$$307 \cdot 43 - 1 = 20 \cdot 660$$

og $660 \,|\, 307 \cdot 43 - 1$. Dvs

$$307 \cdot 43 \equiv 1 \,(\mathrm{mod}\, 660).$$

c) Dekrypter meldingen 028 018 675 129.

Svar: Vi har $p = 23$ og $q = 31$ og $(p-1)(q-1) = 660$. Fra oppgave b) ses at $307 \cdot 43 \equiv 1 \,(\mathrm{mod}\, 660)$. Da er $d = 307$ nøkkel for dekoding. Vi har at $d = 256 + 32 + 16 + 2 + 1$ og derfor er $28^d = 28^{256}28^{32}28^{16}28^{2}28$ etc

$$\begin{aligned} 28^2 = (28^1)^2 &\equiv 71 \,(\mathrm{mod}\, 713) \\ 28^4 = (28^2)^2 &\equiv 50 \,(\mathrm{mod}\, 713) \\ 28^8 = (28^4)^2 &\equiv 361 \,(\mathrm{mod}\, 713) \\ 28^{16} = (28^8)^2 &\equiv 555 \,(\mathrm{mod}\, 713) \\ 28^{32} = (28^{16})^2 &\equiv 9 \,(\mathrm{mod}\, 713) \\ 28^{64} = (28^{32})^2 &\equiv 81 \,(\mathrm{mod}\, 713) \\ 28^{128} = (28^{64})^2 &\equiv 144 \,(\mathrm{mod}\, 713) \\ 28^{256} = (28^{128})^2 &\equiv 59 \,(\mathrm{mod}\, 713) \end{aligned}$$

$$28^d = 28^{256}28^{32}28^{16}28^{2}28 \equiv 59 \cdot 9 \cdot 555 \cdot 71 \cdot 28 \equiv 14 \,(\mathbf{mod}\, 713)$$

$$
\begin{aligned}
18^2 = (18^1)^2 &\equiv 324 \,(\mathrm{mod}\, 713) \\
18^4 = (18^2)^2 &\equiv 165 \,(\mathrm{mod}\, 713) \\
18^8 = (18^4)^2 &\equiv 131 \,(\mathrm{mod}\, 713) \\
18^{16} = (18^8)^2 &\equiv 49 \,(\mathrm{mod}\, 713) \\
18^{32} = (18^{16})^2 &\equiv 262 \,(\mathrm{mod}\, 713) \\
18^{64} = (18^{32})^2 &\equiv 196 \,(\mathrm{mod}\, 713) \\
18^{128} = (18^{64})^2 &\equiv 627 \,(\mathrm{mod}\, 713) \\
18^{256} = (18^{128})^2 &\equiv 266 \,(\mathrm{mod}\, 713)
\end{aligned}
$$

$$18^d = 18^{256}18^{32}18^{16}18^2 18 \equiv 266 \cdot 262 \cdot 49 \cdot 324 \cdot 18 \equiv 9 \,(\mathbf{mod}\, 713)$$

Hopper over de tilsvarende utregningene for de neste kodene. Klarteksten er 14 9 3 5 'NICE'.

Oppgave 2

Jeg har kryptert en tekst med RSA. Min offentlige nøkkel er $(n, d) = (209, 7)$. Min private nøkkel (n, e) får dere selvsagt ikke vite. Finn klarteksten til den krypterte teksten i fellesskap, hele klassen kan samarbeide om dere vil. Hvert tall er en bokstav. Legg merke til at noen a kodene gjentas. De representerer samme bokstav. Om noen ønsker å lage et dataprogram for å finne teksten så anbefaler jeg at maks 3 studenter jobber sammen på denne oppgaven.

24	159	186	121	100	90	186	188	100	143
172	117	186	50	143	100	36	186	36	158
118	152	118	186	121	100	90	186	36	3
143	117	186	117	100	186	141	100	99	186
117	158	118	143	186	51	117	186	188	100
118	191	143	172	117	186	21	3	117	117
118	152	186	36	158	51	66	158	186	206
3	117	158	186	121	100	90	186	117	3
50	118	8							

Jeg har brukt ascii-koder som er gjengitt i tabellen:

A	65	a	97	O	79	o	111
B	66	b	98	P	80	p	112
C	67	c	99	Q	81	q	113
D	68	d	100	R	82	r	114
E	69	e	101	S	83	s	115
F	70	f	102	T	84	t	116
G	71	g	103	U	85	u	117
H	72	h	104	V	86	v	118
I	73	i	105	W	87	w	119
J	74	j	106	X	88	x	120
K	75	k	107	Y	89	y	121
L	76	l	108	Z	90	z	122
M	77	m	109	blank	32	.	46
N	78	n	110	'	180	,	44

Svar: Dekryptering skjer på samme måte som dekrypteringen i oppgave 1c). Som eksempel ser vi på dekoding av første kode som er 24.

$$\begin{aligned} 24^2 = (24^1)^2 &\equiv 158 \,(\mathrm{mod}\, 209) \\ 24^4 = (24^2)^2 &\equiv 93 \,(\mathrm{mod}\, 209) \end{aligned}$$

$$24^d = 24^4 24^2 24 \equiv 93 \cdot 158 \cdot 24 \equiv 73 \,(\mathbf{mod}\, 209)$$

Bokstaven er 'I'

$$\begin{aligned} 159^2 = (159^1)^2 &\equiv 201 \,(\mathrm{mod}\, 209) \\ 159^4 = (159^2)^2 &\equiv 64 \,(\mathrm{mod}\, 209) \end{aligned}$$

$$159^d = 159^4 159^2 159 \equiv 201 \cdot 64 \cdot 159 \equiv 102 \,(\mathbf{mod}\, 209)$$

Bokstaven er 'f'

$$\begin{aligned} 159^2 = (159^1)^2 &\equiv 201 \,(\mathrm{mod}\, 209) \\ 159^4 = (159^2)^2 &\equiv 64 \,(\mathrm{mod}\, 209) \end{aligned}$$

$$159^d = 159^4 159^2 159 \equiv 201 \cdot 64 \cdot 159 \equiv 102 \,(\mathbf{mod}\, 209)$$

Bokstaven er 'f'

$$\begin{aligned} 186^2 = (186^1)^2 &\equiv 201 \,(\mathrm{mod}\, 209) \\ 186^4 = (186^2)^2 &\equiv 64 \,(\mathrm{mod}\, 209) \end{aligned}$$

$$186^d = 186^4 186^2 186 \equiv 199 \cdot 111 \cdot 186 \equiv 32 \,(\mathbf{mod}\, 209)$$

Bokstaven er ' ' (mellomrom)

Fasit:

> If you don't know where you want to go, then it doesn't matter which path you take.

Oppgave 3

Privat og offentlig nøkkel er den samme som i oppgave 1. Finn den private nøkkelen (n, e).

Svar. Knekk nøkkelen ved å faktorisere $209 = pq$. Finn så en multiplikativ invers til 7 modulo $(p-1)(q-1)$. Detaljene er de samme som i oppgave 1b). Svaret er $p = 11$ og $q = 19$. $(p-1)(q-1) = 180$. Euklids utvidede algoritme gir $d = 103$. Detaljene er utelatt.

Oppgave 4

Test ut Diffie-Hellman nøkkelutveksling med $p = 29$ og en medstudent (dvs. bruk denne metoden til å lage dere en felles hemmelig nøkkel). Skriv ned alle utregninger og sjekk at dere sitter igjen med samme nøkkel til slutt. Du kan lese om Diffie-Hellmann i for eksempel foilene som ligger i samme mappe som denne oppgaven.

Oppgave 5

Se filen med overskrift Ekstra oppgaver som ligger på blackboard. Løs oppgave X