Exercise 5

Module 1 - Introduction to Cryptography and Data Security

Knut Lucas Andersen
Master Applied Information Security
isits AG International School of IT Security

June 26, 2017

Contents

1 Square and Multiply **3**
a) x = 5; e = 54; m = 151 3
b) x = 8; e = 127; m = 151 3
c) x = 7; e = 52; m = 197 4
d) x = 9; e = 44; m = 197 4

2 RSA Ver- und Entschlüsselung **4**
a) p = 19; q = 43; e = 67; x = 143 4
b) p = 27; q = 37; e = 117; x = 666 4
c) p = 23; q = 31; d = 449; y = 25 4

3 Angrif auf RSA **5**

1 Square and Multiply

a) x = 5; e = 54; m = 151

Fast exponentiation - $e_b = 11011_2$:

$$\begin{aligned}
x \cdot x = x^2 \quad &\Rightarrow \quad (x^{1_2})^2 = x^{10_2} \\
x^2 \cdot x = x^3 \quad &\Rightarrow \quad x^{10_2} \cdot x^{1_2} = x^{11_2} \\
x^3 \cdot x^3 = x^6 \quad &\Rightarrow \quad (x^{11_2})^2 = x^{110_2} \\
x^6 \cdot x^6 = x^{12} \quad &\Rightarrow \quad (x^{110_2})^2 = x^{1100_2} \\
x^{12} \cdot x = x^{13} \quad &\Rightarrow \quad x^{1100_2} \cdot x^{1_2} = x^{1101_2} \\
x^{13} \cdot x^{13} = x^{26} \quad &\Rightarrow \quad (x^{1101_2})^2 = x^{11010_2} \\
x^{26} \cdot x = x^{27} \quad &\Rightarrow \quad x^{11010_2} \cdot x^{1_2} = x^{11011_2} \\
x^{27} \cdot x^{27} = x^{54} \quad &\Rightarrow \quad (x^{11011_2})^2 = x^{110110_2}
\end{aligned} \tag{1}$$

b) x = 8; e = 127; m = 151

Fast exponentiation - $e_b = 1111111$:

$$\begin{aligned}
x \cdot x = x^2 \quad &\Rightarrow \quad (x^{1_2})^2 = x^{10_2} \\
x^2 \cdot x = x^3 \quad &\Rightarrow \quad x^{10_2} \cdot x^{1_2} = x^{11_2} \\
x^3 \cdot x^3 = x^6 \quad &\Rightarrow \quad (x^{11_2})^2 = x^{110_2} \\
x^6 \cdot x = x^7 \quad &\Rightarrow \quad x^{110_2} \cdot x^{1_2} = x^{111_2} \\
x^7 \cdot x^7 = x^{14} \quad &\Rightarrow \quad (x^{111_2})^2 = x^{1110_2} \\
x^{14} \cdot x = x^{15} \quad &\Rightarrow \quad x^{1110_2} \cdot x^{1_2} = x^{1111_2} \\
x^{15} \cdot x^{15} = x^{30} \quad &\Rightarrow \quad (x^{1111_2})^2 = x^{11110_2} \\
x^{30} \cdot x = x^{31} \quad &\Rightarrow \quad x^{11110_2} \cdot x^{1_2} = x^{11111_2} \\
x^{31} \cdot x^{31} = x^{62} \quad &\Rightarrow \quad (x^{11111_2})^2 = x^{111110_2} \\
x^{62} \cdot x = x^{63} \quad &\Rightarrow \quad x^{111110_2} \cdot x^{1_2} = x^{111111_2} \\
x^{63} \cdot x^{63} = x^{126} \quad &\Rightarrow \quad (x^{111111_2})^2 = x^{1111110_2} \\
x^{126} \cdot x = x^{127} \quad &\Rightarrow \quad x^{1111110_2} \cdot x^{1_2} = x^{1111111_2}
\end{aligned} \tag{2}$$

c) x = 7; e = 52; m = 197

Fast exponentiation - $e_b = 110100$:

$$\begin{aligned} x \cdot x = x^2 \quad &\Rightarrow \quad (x^{1_2})^2 = x^{10_2} \\ x^2 \cdot x = x^3 \quad &\Rightarrow \quad x^{10_2} \cdot x^{1_2} = x^{11_2} \\ x^3 \cdot x^3 = x^6 \quad &\Rightarrow \quad (x^{11_2})^2 = x^{110_2} \\ x^6 \cdot x^6 = x^{12} \quad &\Rightarrow \quad (x^{110_2})^2 = x^{1100_2} \\ x^{12} \cdot x = x^{13} \quad &\Rightarrow \quad x^{1100_2} \cdot x^{1_2} = x^{1101_2} \\ x^{13} \cdot x^{13} = x^{26} \quad &\Rightarrow \quad (x^{1101_2})^2 = x^{11010_2} \\ x^{26} \cdot x^{26} = x^{52} \quad &\Rightarrow \quad (x^{11010_2})^2 = x^{110100_2} \end{aligned} \tag{3}$$

d) x = 9; e = 44; m = 197

$$\begin{aligned} x \cdot x = x^2 \quad &\Rightarrow \quad (x^{1_2})^2 = x^{10_2} \\ x^2 \cdot x^2 = x^4 \quad &\Rightarrow \quad (x^{10_2})^2 = x^{100_2} \\ x^4 \cdot x = x^5 \quad &\Rightarrow \quad x^{100_2} \cdot x^{1_2} = x^{101_2} \\ x^5 \cdot x^5 = x^{10} \quad &\Rightarrow \quad (x^{101_2})^2 = x^{1010_2} \\ x^{10} \cdot x = x^{11} \quad &\Rightarrow \quad x^{1010_2} \cdot x^{1_2} = x^{1011_2} \\ x^{11} \cdot x^{11} = x^{22} \quad &\Rightarrow \quad (x^{1011_2})^2 = x^{10110_2} \\ x^{22} \cdot x^{22} = x^{44} \quad &\Rightarrow \quad (x^{10110_2})^2 = x^{101100_2} \end{aligned} \tag{4}$$

2 RSA Ver- und Entschlüsselung

a) p = 19; q = 43; e = 67; x = 143

$$\begin{aligned} n = p \cdot q = 19 \cdot 43 = 817 \\ \varnothing(n) = (p-1)(q-1) = (19-1)(43-1) \Rightarrow 18 \cdot 42 = 756 \\ K_{pub} = (n, e) = (817, 67) \\ x^e \ mod \ n = 143^{167} \ mod \ 817 \end{aligned} \tag{5}$$

b) p = 27; q = 37; e = 117; x = 666

$$\begin{aligned} n = p \cdot q = 27 \cdot 37 = 999 \\ \varnothing(n) = (p-1)(q-1) = (27-1)(37-1) \Rightarrow 26 \cdot 36 = 936 \\ K_{pub} = (n, e) = (999, 117) \\ x^e \ mod \ n = 666^{999} \ mod \ 817 \end{aligned} \tag{6}$$

c) p = 23; q = 31; d = 449; y = 25

$$\begin{aligned} n = p \cdot q = 23 \cdot 31 = 713 \\ \varnothing(n) = (p-1)(q-1) = (23-1)(31-1) \Rightarrow 22 \cdot 30 = 660 \\ K_{priv} = (d) = 449 \\ y^d \ mod \ n = 25^{449} \ mod \ 713 \end{aligned} \tag{7}$$

3 Angrif auf RSA

-