

Some hints/solutions to exercises

TMA4160 Cryptography, autumn 2007

Exercise 1:

Task 5: Hint: In how many ways can you choose the first column of the matrix?
What about the second one? Etc.

Exercise 2:

Task 4: The keyword is "vigenere".

1.7: 240, 4000, 1029000.

1.15: a) $\begin{pmatrix} 11 & 15 \\ 1 & 20 \end{pmatrix}$. b) $\begin{pmatrix} 25 & 11 & 22 \\ 10 & 13 & 4 \\ 17 & 24 & 1 \end{pmatrix}$.

Exercise 3:

Task 1: a) $x \equiv 23 \pmod{30}$. b) $x \equiv 221 + 97097 \cdot a \pmod{1068067}$, for $a = 0, 1, 2, \dots, 10$.
c) No solution.

Task 2 (5.5): Hint: Use the Chinese Remainder Theorem. $\chi(2, 2, 3) = 17$.

Task 3 (5.8): The smallest primitive element modulo 97 is 5.

Task 5 (5.11): b) Modified RSA: $a = 67$. Original RSA: $a = 2407$.

Exercise 4:

Task 1: c) The maximum message length is $\lfloor \log_b n \rfloor$.

5.15: b) The plaintext is "vanilla".

5.16: b) $x = 15001$.

Exercise 5:

5.22: a) Hint: Use property 3 on p. 183 in Stinson's book.

5.25: $262063 = 503 \cdot 521$. $9420457 = 4007 \cdot 2351$.

5.26: $262063 = 503 \cdot 521$. $9420457 = 4007 \cdot 2351$. $181937053 = 14683 \cdot 12391$.

5.27: $256961 = 293 \cdot 877$.

6.3: The discrete logarithm is 40007.

Exercise 6:

6.4: a) Hint: Use the binomial theorem, and recall that $a \equiv 1 \pmod{bc} \Rightarrow a \equiv 1 \pmod{b}$ and $a \equiv 1 \pmod{c}$.

c) Hint: Look at 3^{29} .

6.6: a) $2^{32} \pmod{227} = 2^4 \cdot 11$. $2^{40} \pmod{227} = 2 \cdot 5 \cdot 11$. $2^{59} \pmod{227} = 2^2 \cdot 3 \cdot 5$.
 $2^{156} \pmod{227} = 2^2 \cdot 7$.

b) $\log 3 = 46$. $\log 5 = 11$. $\log 7 = 154$. $\log 11 = 28$.

c) $\log 173 = 26$.

6.10: $x^5 + x^3 + 1$ is irreducible.

6.11: a) $(x^4 + x^2) \cdot (x^3 + x + 1) = x^3$.

b) $(x^3 + x^2)^{-1} = x^2 + x + 1$.

c) $x^{25} = x^4 + x^3 + 1$.

Exercise 7:

Task 1: a) $2P = (10, 6)$, $5P = (1, 0)$, $10P = \infty$.

b) There are 10 points on the curve.

c) The points are: $(1, 0)$, $(5, 2)$, $(5, 9)$, $(8, 2)$, $(8, 9)$, $(9, 2)$, $(9, 9)$, $(10, 5)$, $(10, 6)$, ∞ .

Task 2 a) Hint: Recall that $\mathbf{Z}_m \times \mathbf{Z}_n \simeq \mathbf{Z}_{mn}$ iff $\gcd(m, n) = 1$. The groups are: \mathbf{Z}_{100} , $\mathbf{Z}_2 \times \mathbf{Z}_{50}$, $\mathbf{Z}_5 \times \mathbf{Z}_{20}$ and $\mathbf{Z}_{10} \times \mathbf{Z}_{10}$. The maximal orders are 100, 50, 20 and 10, respectively.

Task 3 The substitution $x = y - 3^{-1}c$ works.

Task 4 Hint: Use Hasse's Theorem and Theorem 6.1 (both on page 261 in Stinson's book).

Exercise 8:

Task 1: a) The maximal order is 2.

b) Hint: Use the result from a).

c) An example is the curve $y^2 = x^3 + 5x + 7 = (x - 6)(x - 7)(x - 9)$ over \mathbf{Z}_{11} .

Task 2 (6.13) a) Hint: You may use the function `msolve` in Maple to solve this problem. There are 72 points on the curve.

b) Hint: You may use the function `msolve` in Maple to factorize $x^3 + x + 28$ over \mathbf{Z}_{71} , and then use the result from Task 1 a). c) Hint: Given that $(E, +)$ is not cyclic, you can use Theorem 6.1 (on page 261 in Stinson's book) to show that $(E, +) \simeq \mathbf{Z}_2 \times \mathbf{Z}_{36}$. The maximal order is 36. An element of this order is $(0, 1)$.

Task 4 (1.18) For $(0, 0, 0, 0)$ the period is 1. For any other initialization vector the period is 5.

Exercise 9:

Task 3: Olga can impersonate Bob as follows: Assume that r_1 and y_1 , produced by Bob, are observed from a previous session. Then Olga sends $(Cert(Bob), r_1, y_1)$ to Alice, and upon receiving $(Cert(Alice), r_2, y_2, y_3)$ from Alice, Olga sends $(Cert(Alice), r_2, y_2)$ to Bob, pretending to be Alice. Note that Bob's response to this message contains an element which Olga may send to Alice as an appropriate final message y_4 .

Exercise 10:

Task 1: a) Hint: Use that α is a primitive element.
b) $k = 56429$, $a = 9871$.

Task 2: $x=19012507151504022505$

Task 3: Hint: Note that, with these primes, we have $n_b < n_a$, so the encryption function is no longer injective (1-1).