Model Answer + Grading Rubric

Answer of exercise 1

1) The decryption result of each block c_i in each of the given scenarios are summarized in the following table:

01,00

	m_1	m_2	m_3	m_4	m_5
Scenario (a)	✗erroneous	✓correct	✗erroneous	✓correct	✓correct
Scenario (b)	✗erroneous	✗erroneous	✗erroneous	✗erroneous	✗erroneous
Scenario (c)	✓correct	✓correct	✗erroneous	✗erroneous	✓correct
Scenario (d)	✗erroneous	✓correct	✓correct	✗erroneous	✓correct

2) Comparison of ECB, CBC and CTR modes of operation according to 3 criteria of my choice.:

03,00

	ECB	CBC	CTR
Identical blocks in plaintext	Identical blocks in cyphertext	Different blocks in cyphertext	Different blocks in cyphertext
Identical plaintexts	Identical cyphertexts	Different cyphertexts	Different cyphertexts
Error propagation	No	Limited (2 blocks)	No
Parallelism	Encryption and Decryption	Only Decryption	Encryption and Decryption
Ciphertext block loss	All received blocks are correctly decrypted	Decryption is impossible after a lost block	All received blocks are correctly decrypted

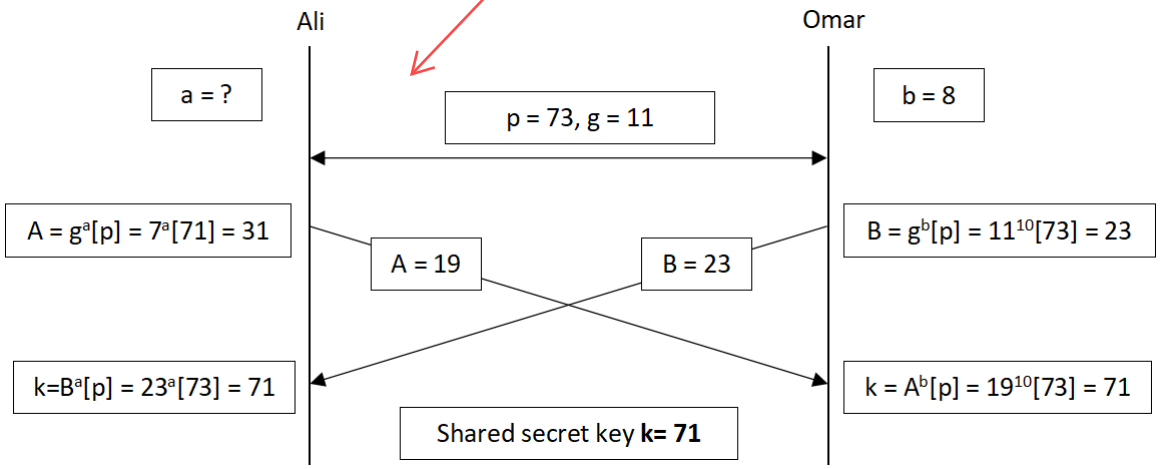
Answer of exercise 2

1) ***Omar*** should send to Ali the value $B = g^b \mod p = 11^{10} \mod 73$. Hence $B = 23$.

01,00

2) Their shared secret value is $k = 71$.

03,00



3) In the general case, it is **hard** (impossible in practice in a reasonable amount of time) to figure out ***Ali***'s secret exponent since we must solve the hard mathematical discrete logarithm problem.

02,00

Answer of exercise 3

1) The RSA module $n = p \times q = 137 \times 151 = 20687$

01,00

The Euler's totient is $\varphi(n) = (p-1)(q-1) = 136 \times 150 = 2^4 \times 3 \times 5^2 \times 17 = 20400$.

01,00

2) The smallest value of the encryption exponent e usable such that $e \leq 10$, is $e = 7$ because $PGCD(7, 20400) = 1$ and:

01,00

- $\forall i \in \{2, 4, 6, 8, 10\} : \ PGCD(i, 20400) \neq 1$.

- $PGCD(3, 20400) = 3 \neq 1$.
- $PGCD(5, 20400) = 5 \neq 1$.
- $PGCD(7, 3016) = 1$.

01,00

3) ***Ali***'s public key is $(n, e) = (20687, 7)$.
The decryption exponent d must satisfy $e \times d \equiv 1 \mod \varphi(n)$ and using the extended Euclidean algorithm, we obtain:
$20400 \times (-3) + 7 \times 8743 = 1$. The decryption exponent is: $d = 8743 \mod 20400$.

i	r_i	q_i	α_i	β_i
1	20400	–	1	0
2	7	2914	0	1
3	2	3	1	-2914
4	1	2	-3	8743
5	0	–	–	–

01,00

Ali's private key is $(n, d) = (20687, 8743)$.

01,00

4) The cryptogram c corresponding to the plaintext $m = 16$:
$c = m^e \mod n = 16^7 \mod 20687 = 944$. Hence, $c = 944$.

5) The plaintext m corresponding to the cryptogram $c = 2$:
$m = c^d \mod n = 2^{8743} \mod 20687 = 2^{5100} \times 2^{3643} \mod 20687 = 2^{3643} \mod 20687 = 2^{1000} \times 2^{1000} \times 2^{1000} \times 2^{643} \mod 20687 = 17181^3 \times 2^{643} \mod 312$. Hence, $m = 19970$.

01,00