Written exam in cryptography

Name and surname:

Exercise	1	2	3	4	Σ
Points					

Instructions

- Write on white A4 sheets of paper and do not use ordinary pencil or red pen.
- Start writing each exercise on a new page and mark the beginning of each subtask.
- Calculators are allowed for addition, multiplication and exponentiation modulo n (unless otherwise required). Other calculations must be worked out step by step. Penalty: 50%.
- Give proper reasons for your statements. Write comments on the calculations. Penalty: 50%.

Exercises

1. [25 POINTS] RSA protocol, attacks on RSA, prime factorization problem
   (a) [10 POINTS] Alice has the RSA public key $(n, e) = (589, 23)$. Decide whether any of the following keys (n, d) is Alice's private key: $(589, 45)$, $(589, 47)$, $(589, 49)$. Alice received a message $b = 10$, decrypt this message.
   (b) [10 POINTS] The public and private key-pair is known for the RSA protocol: $(n, e) = (7811, 17)$, $(n, d) = (7811, 449)$. Use the insider attack to factorize the module $n = 7811$. (Note: This is not brute force factoring, but factoring based on knowledge of a multiple of $\varphi(n)$!)
   (c) [5 POINTS] Prove that knowing $\varphi(n)$ allows to factorize the module n of the RSA protocol.
2. [25 POINTS] Diffie-Hellman key establishment, ElGamal protocol, discrete logarithm problem
   (a) [5 POINTS] Verify that the element $a = 124$ is a generator of the cyclic group $\mathbb{Z}_{131}^*$.
   (b) [10 POINTS] Use the Baby step/giant step algorithm to compute $\mathrm{dlog}_{124}(90)$ in $\mathbb{Z}_{131}^*$.
   (c) [10 POINTS] The ElGamal encryption protocol uses the cyclic group $\mathbb{Z}_{131}^*$ with the generator $a = 124$. Alice's public key is $e = 90$. Alice received a message $(c, \bar{m}) = (73, 103)$, decrypt this message.
3. [25 POINTS] Primality tests, generating random primes
   (a) [5 POINTS] Use the Fermat test to check if $n = 377$ is prime. Choose two witnesses: $a = 12$, $b = 52$.
   (b) [5 POINTS] In which case can be an element, which proves in the Fermat test that n is not prime, used for factoring n? Use calculations from the previous subtask to factorize $n = 377$.
   (c) [10 POINTS] Find the set of all false Fermat witnesses for primality of $n = 377$.
   (d) [5 POINTS] Does the witness $a = 12$ reveal the compositeness of $n = 377$ if we use the Miller-Rabin test?
4. [25 POINTS] Subexponential algorithms for discrete logarithm or for factoring integers
   (a) [5 POINTS] In the group $\mathbb{Z}_{19}^*$, we know the representation $(s, t) = (6, 8)$ of the element 1 with respect to the generator $a = 2$ and the element $b = 7$. Calculate $\mathrm{dlog}_2(7)$ in $\mathbb{Z}_{19}^*$.
   (b) [15 POINTS] $G = \langle 16 \rangle$ is a cyclic subgroup of order $q = 37$ in the group $\mathbb{Z}_{149}^*$. Use the algorithm SEDL to compute $\mathrm{dlog}_{16}(36)$ in G, choose the smoothness parameter $y = 3$.
   (c) [5 POINTS] Let $G = \langle a \rangle$ be a subgroup of order q in the group $\mathbb{Z}_p^*$, where p is a prime. Prove that $\mathrm{dlog}_a(b)$ is defined if and only if $b^q = 1$ in $\mathbb{Z}_p^*$.