

Cryptology, homework sheet 5

Due 6 October 2026, 13:30

Team up in groups of two or three to hand in your homework. We do not have capacity to correct all homeworks individually.

For this exercise you can use Sage for computations modulo p, q and n , including exponentiations. You may not use the built-in function for solving the DLP but follow the algorithm specified. Make sure to document what you type and what the answers are.

1. This is a continuation of exercise 2 from HW sheet 4. See there for details of the regular ElGamal signature system. This exercise uses the same signature scheme, but it puts $(x(R), s)$ as the signature instead of (R, s) and then checks if $x(w_1P + w_2P_A) = x(R)$.

Show how evil Alice can pick her secret key a dependent on two fixed, given messages m_1 and m_2 , so that she can later pretend that a signature $(x(R), s)$ on m_1 was a signature on m_2 . Note, this means *the same* signature $(x(R), s)$ satisfies the verification equation for m_1 and m_2 .

State a as an expression in m_1, m_2 , and the group order ℓ .

Hint: You will also fix r for that signature at KeyGen time.

5 points

2. For RSA Bob uses public key $(n, e) = (396553, 17)$. His secret key is a CRT key using $p = 541$ and $q = 733$.

- (a) Compute the full secret key (n, p, q, d_p, d_q, u) , where $u \equiv p^{-1} \pmod q$ is then used in RSA-CRT to compute $m \equiv m_p + pu(m_q - m_p) \pmod n$.

1.5 points

- (b) Perform one round of the Fermat test with base $a = 2$ to test whether p is prime.

1 point

- (c) Decrypt ciphertext $c = 234040$ using the CRT method and verify your result by reencrypting it.

Make sure to document your computation, i.e., state the values for $c_p, m_p, \dots$

3.5 points

3. **Combination of hash functions.** Are the following claims true or false? Either present a proof by giving a reduction as in the lecture or a counter example.

- (a) Let $h : \{0, 1\}^n \times \{0, 1\}^n \rightarrow \{0, 1\}^n$ be an efficient keyed permutation. Let $H = h \circ h$ be the permutation resulting from applying h twice with the same key, i.e., $H(k, m) = h(k, h(k, m))$.

Claim: If h is preimage resistant, H is preimage resistant.

2 points

- (b) Let $h_1 : \{0, 1\}^{n_1} \times \{0, 1\}^{\ell(n_1)} \rightarrow \{0, 1\}^{n_1}$ and $h_2 : \{0, 1\}^{n_2} \times \{0, 1\}^{n_1} \rightarrow \{0, 1\}^{n_2}$ be hash functions.

Claim: The combined hash function $H : \{0, 1\}^{n_1+n_2} \times \{0, 1\}^{\ell(n_1)} \mapsto \{0, 1\}^{n_2}; ((k_1, k_2), m) \mapsto h_2(k_2, h_1(k_1, m))$ is collision resistant if at least one of h_1 and h_2 is collision resistant and h_2 is not constant.

2 points