

Exercise 2 (21.11.2023)

Test

1. The birthday attack on hash function finds
☐ preimage ☐ 2nd preimage ☐ collision
2. HMAC processes each block of the input message twice.
☐ yes ☐ no
3. Let's compare the signature length of DSA and ElGamal scheme, while requiring the same security level. Signatures in DSA are
☐ shorter ☐ longer ☐ equal length
4. PBKDF2 uses, beside a password, a salt as a input.
☐ yes ☐ no
5. The plaintext in Regev scheme based on LWE problem (Learning with Errors) over \mathbb{Z}_q is selected from the set
☐ $\{0, 1\}$ ☐ \mathbb{Z}_q ☐ $\{-\frac{q-1}{2}, \dots, \frac{q-1}{2}\}$
6. Merkleho-Damgård construction of hash function guarantees that the resulting hash function is collision resistant if the compression function is collision resistant.
☐ yes ☐ no
7. The signature scheme RSA PKCS#1 v1.5 is
☐ deterministic ☐ randomized
8. We expect that the more computationally complex operation in the Merkle signature scheme (MSS) is
☐ verification ☐ signing
9. A deficiency of PBKDF2 function (when used for storing passwords) in relations to dictionary attacks is
☐ low memory complexity
☐ impossibility to parallelize the computation
☐ limited output length
10. The Schnorr signature scheme is immune to random message forgery.
☐ yes ☐ no
11. McEliece scheme for asymmetric encryption is not secure if the underlying error-correcting code corrects at most 1 error.
☐ yes ☐ no
12. Hellman table for finding password corresponding to a given hash. Transformations from hash values to passwords are
☐ distinct for each row and column ☐ distinct for each row ☐ the same for each row and column
13. Let H be a collision-resistant hash function. Then $G(x) = H(x) \oplus H(\bar{x})$ is collision-resistant.
☐ yes ☐ no
14. Merkle signature scheme uses a tree with depth k (a root has depth 0). The scheme allows signing
☐ 1 message ☐ k messages ☐ 2^k messages ☐ $2^{k+1} - 1$ messages
15. Using salt when storing passwords has the following goal:
☐ slow down hash computation in dictionary attack
☐ prevent brute-force attack
☐ slow down an attacker in guessing passwords on-line
☐ prevent precomputation of hashes in advance.
16. The complexity of decryption in Regev scheme (based on LWE problem, with private key/vector length n) is

☐ $O(\log n)$ ☐ $O(n)$ ☐ $O(n \log n)$ ☐ $O(n^2)$

17. Let h be the length of a hash function output and k be the key length. Then the output length of HMAC is

☐ h ☐ $h + k$ ☐ $2h$ ☐ $2h + k$ ☐ none of the other answers

Problems

1. (Curveball 2020) A public key of a user in ECDSA scheme is $Q = dG$, where $d \in \mathbb{Z}_n^*$ is a private key (the elliptic curve subgroup generated by G has order n , where n is a prime number). Show anyone can forge a signature for any message m , if the recipient accepts arbitrary G' as a parameter of the scheme (other parameters are not modified).
2. Let E be a block cipher (e.g. AES-128). Predpokladajme, že dĺžka správy je vždy násobkom dĺžky bloku (označme správu m rozdelenú na bloky takto: $m = m_1, m_2, \dots, m_n$). Zdôvodnite, prečo nasledujúce konštrukcie nie sú vhodné ako MAC:
 - a) $H_k(m) = (c_0, c_n)$, kde c_n je posledný blok získaný šifrovaním m pomocou E_k v CFB móde a c_0 je náhodne zvolený IV,
 - b) $G_k(m) = E_{m_n}(\dots E_{m_2}(E_k(m_1)) \dots)$, kde predpokladáme, že v E je dĺžka bloku zhodná s dĺžkou kľúča,
 - c) $F_k(m) = E_k(m_1) \oplus E_k(E_k(m_2)) \oplus \dots \oplus E_k^n(m_n)$.
3. Decide and justify the security of the following variants of Schnorr signature scheme (parameters are the same as in original scheme; certainly, the verification equation must be adjusted accordingly):
 - a) The value s is modified: $s = k + r + x \bmod q$ (r remains unchanged).
 - b) The value s is modified: $s = k - rx \bmod q$ (r remains unchanged).
4. We modify Goldreich signature scheme so that in the tree each non-leaf (parent) node has 4 children. We sign the 256-bit hash of a message.
 - a) Describe how signing and verification will be performed in the new scheme.
 - b) Compare the lengths of public key, private key, and signature in the original and the new scheme. For OTS scheme used in the construction we denote by v the length of the public key, by s the length of the private key, and by p the length of the signature.
 - c) Compare the time complexity of signing in both schemes. Let g be a complexity single OTS scheme generation, and let f be a complexity of signing in a OTS scheme.
5. Let g be a generator of the group (\mathbb{Z}_p^*, \cdot) , for a large prime number p . We divide the message m into blocks $m = m_1, m_2, \dots, m_n$, where each $m_i \in \mathbb{Z}_p$. Decide and justify the collision-resistance of the following hash functions:
 - a) $H(m) = h_n$, kde $h_i = g^{h_{i-1} + m_i}$ a $h_0 = 0$;
 - b) $H(m) = h_n$, kde $h_i = g^{m_i} \cdot h_{i-1}$ a $h_0 = 2020$.
6. The attacker knows the ciphertext $c = mG' + e$ in McEliece scheme, where $\text{wt}(e) \leq t$. Let's assume the attacker can distinguish for a ciphertext c' whether there at most t errors in c' and decryption results in m (situation A), or there is more than t errors or decrypted text is not m (situation B). Describe and justify how the attacker with access to the oracle distinguishing situations A and B can remove the error vector e from c , i.e. get $x = mG'$. Calculate the number of required oracle queries in the worst case.
Hint: Split the attack into two parts. In the first one compute c^* from c , such that c^* has exactly $t + 1$ errors with respect to x .