Assignment 4: COMP6453 2024 T2

This set consists of 3 questions with a total marks of 60.

1 DSA Variant

Consider a variant of DSA in which the message space is Z_q and the hash function H is omitted. Signing and verification keys are the same as we learnt in class. The signing algorithm is as given below.

Let message be $m \in Z_q$. Signer chooses $k \xleftarrow{R} Z_q^*$, computes $r = (g^k \mod p) \mod q$, computes $s = (m + xr).k^{-1} \mod q$, outputs signature $\sigma = (r, s)$.

Show that this variant is not secure.

Marks: 10 marks

2 RSA Signature Variant

Consider the following RSA trapdoor permutation where every party uses the same modulus $n = pq$. Every party i is assigned a public exponent $e_i \in \mathbb{Z}$ and a private exponent $d_i \in \mathbb{Z}$ such that $e_i.d_i = 1 \mod \phi(n)$.

To sign a message $m \in \mathcal{M}$, Alice constructs the signature $\sigma_a \leftarrow H(m)^{d_a} \in \mathbb{Z}$ where $H : \mathcal{M} \to \mathbb{Z}_n^*$ is a hash function.

The aim of this exercise is to show that this is completely insecure: Bob can use his secret key d_b to sign messages on behalf of Alice.

(a) Show that Bob can use his public-private key pair (e_b, d_b) to obtain a multiple of $\phi(n)$. Let us denote that integer by V .

(b) Now, suppose Bob knows Alice's public key e_a. Show that for any message $m \in \mathcal{M}$, Bob can compute $\sigma \leftarrow H(m)^{1/e_a} \in \mathbb{Z}_n$. In other words, Bob can invert Alice's trapdoor permutation and obtain her signature on m.

Hint: First, suppose e_a is relatively prime to V . Then Bob can find an integer d such that $de_a = 1 \bmod V$. Show that d can be used to efficiently compute σ. Next, show how to make your algorithm work even if e_a is not relatively prime to V.

Marks

- Part (a): 5 marks

- Part (b): 10 marks
- Total: 15 marks

3 Blockchain

For each of the blockchains below study documents/specs/code available on the web to answer the following questions:

- Bitcoin
- Ethereum
- Cardano
- Solana
- Algorand

Write the following for each of the above blockchains.

1. Block Structure: What fields are present and what are the implications.
2. Transaction Structure: What fields are present and what are the implications.
3. State Structure: For example, Ethereum uses a Merkle Patricia Trie to state the world state. What are the entries in this state trie?

Marks

- Part (1): 10 marks
- Part (2): 10 marks
- Part (3): 15 marks
- Total: 35 marks

Full Submission

1. Q1: Write answer in a file q1. You can use pdf or txt format.
2. Q2: Write answer in a file q2. You can use pdf or txt format.
3. Q3: Write answer in a file q3. You can use pdf or txt format.
4. Upload a zip file with all three answers. $\langle zid \rangle \langle ass4 \rangle .zip$