COMP6453: Week 8 Answers

1 Textbook RSA Signatures

Textbook RSA encryption gives rise to a digital signature scheme in the following way:

Keygen: Key generation is the same as in textbook RSA encrytion: It chooses two large primes p and q and chooses (e, d) such that $ed \equiv 1 \pmod{\phi}(n)$, where $n = pq$. The public verification key is the pair (n, e) and the private signing key is (n, d). The space of messages you can sign is $\{0, 1, ..., n-1\}$.

Sign: For a message $m \in \{0, ..., n-1\}$, use the secret signing key (n, d) to compute the signature $\sigma = m^d \pmod{n}$.

Verify: For a signature and message $\sigma, m \in \{0, ..., n-1\}$, use the verification key (n, e) to check $\sigma^e = m \pmod{n}$.

This exercise shows textbook RSA signatures are inscure, which is why we need to augment this scheme with the Full Domain Hash Construction, as shown in the lecture.

(i). Let $(n, 3)$ be the public verification key. Forge a signature on the message 8.

Answer:

$\sigma^3 = 8 \pmod{n}$. Thus $\sigma = 2$

(ii). Suppose (n, e) is a verification key. Explain how to create a random message with a forged signature.

Answer:

Sample a random $\sigma \in \{0, 1, ..., n-1\}$ and compute $m = \sigma^e \pmod{n}$. Then σ is a signature for m.

(iii). Suppose you have two messages m, m' and signatures σ, σ' on those messages under the verification key (n, e). Show how to construct a signature on the product $mm' \pmod{n}$.

Answer:

Forgery is just $(\sigma \cdot \sigma')^e = m \cdot m' \pmod{n}$.

2 Diffie Hellman Signature

It is tempting to try to develop a variation on Diffie–Hellman that could be used as a digital signature. Here is one that is simpler than DSA and that does not require a secret random number in addition to the private key:

Public Elements: a prime q, $\alpha < q$ (where α is a primitive root modulo q)

Private Key: X, where $X < q$

Public Key: $Y = \alpha^X \pmod{q}$.

To sign a message M, compute $h = H(M)$, which is the hash of the message. We require that $gcd(h, q-1) = 1$. If not, append the hash to the message and calculate a new hash. Continue this process until a hash is produced that is relatively prime to $(q-1)$. Then calculate Z to satisfy $Z = X \cdot h \pmod{q-1}$. The signature of the message is $\sigma = \alpha^Z$. To verify the signature, a user computes t such that $t \cdot h = 1 \pmod{q-1}$ and verifies $Y = \sigma^t \pmod{q}$.

Show that the scheme is insecure by describing a simple technique for forging a user's signature on an arbitrary message.

Answer:

To sign any message h with $gcd(h, q-1) = 1$, just compute Y^h. Verification function: $Y = \sigma^t$ thus $Y^{h \cdot t} = Y = \sigma^t$. We know that $h \cdot t = 1 \pmod{n}$.

3 Blockchain Explorer

This exercise is to understand how cryptocurrency transactions work.

Open up a browser and use a blockchain explorer to explore transatcions. An example of a blockchain explorer is https://www.blockchain.com/explorer

Check out the following for cryptocurrencies like Bitcoin, Ethrereum, Solana, Cardono, Ripple, Algorand, etc...

1. Read the history
2. Understand block structures
3. Understand transaction structures: inputs, outputs, transaction fees, signatures etc.
4. Hash rates, transaction throughput etc.