CAA 24-25

Exercise Sheet on Asymmetric Cryptography

1 Schnorr Signatures

Schnorr signatures are based on the discrete logarithm problem (either on $\mathbb{Z}_p^*$ or on an elliptic curve). They were patented until 2008.

- **Parameters**: an element g of prime order q in a group G in which the discrete logarithm is hard. A hash function $H : \{0,1\}^* \to \mathbb{Z}_q$
- **Keys**: Private key: $x \in \mathbb{Z}_q$, Public key: $y = g^x$
- **Signing**: to sign a message m,
    1. Draw a random $k \in \mathbb{Z}_q$.
    2. Let $r = g^k$
    3. Let $e = H(r \| m)$
    4. Let $s = k - xe$
    5. Return (s, e).

1. How do you verify the signature?
   Hint: you need to recreate e and verify that it corresponds to the received one.
2. Show how you can recover the private key if the randomness k is reused for signing two different messages.
3. Show how you can recover the private key if the randomness k is incremented by one between each signature.
4. Show how you can recover the private key if the randomness k is doubled between each signature.

2 IND-CPA / IND-CCA Security

1. To secure your system, you are given the choice between an IND-CPA and an IND-CCA cryptosystem. Which one do you choose? Justify.
2. A bad developer decides to fix the seed of RSA-OAEP to 0. Is the result still IND-CCA2 secure? Is it IND-CPA secure? Justify.
3. Show that the El-Gamal encryption is **not** IND-CCA2 secure.