# CAA 24-25

# Exercise Sheet on Asymmetric Cryptography
# Solutions

## 1 Schnorr Signatures

1. We compute $r = g^s y^e$ and we verify that $e == H(r\|m)$.

2. Given two message $m_1$ and $m_2$ and their signatures $(s_1, e_1)$ and $(s_2, e_2)$, we simply compute
$$\frac{s_1 - s_2}{e_2 - e_1} = x$$

3. Given two message $m_1$ and $m_2$ and their consecutive signatures $(s_1, e_1)$ and $(s_2, e_2)$, we have $s_1 = k - xe_1$ and $s_2 = k + 1 - xe_2$ for a $k$. Then,
$$\frac{s_1 - s_2 + 1}{e_2 - e_1} = x$$

4. Given two message $m_1$ and $m_2$ and their consecutive signatures $(s_1, e_1)$ and $(s_2, e_2)$, we have $s_1 = k - xe_1$ and $s_2 = 2k - xe_2$ for a $k$. Then,
$$\frac{2s_1 - s_2}{e_2 - 2e_1} = x$$

## 2 IND-CPA / IND-CCA Security

1. I would choose the IND-CCA cryptosystem. Indeed, an IND-CCA cryptosystem is strictly more secure as an IND-CPA system. An adversary in an IND-CCA system can additionally do chosen ciphertext attacks. Hence, he has more capabilities. Thus, if the system IND-CCA secure, it is protected against a stronger adversary.

2. The system becomes deterministic. Hence, it is neither IND-CCA2 nor IND-CPA secure. To win the IND-CPA (and also the IND-CCA2) game, the adversary chooses two random plaintexts $M_0$ and $M_1$. Upon reception of the ciphertext $y$, he can simply compute the RSA-OAEP encryption of $M_0$ and $M_1$ with the seed fixed to 0 and compare what he obtains with $y$. He can, thus, win the game with probability 1.

3. The El-Gamal encryption is malleable. An adversary wins the IND-CCA2 game in the following way. He selects two random message $M_0$, $M_1$ to be encrypted. Upon

reception of a ciphertext $y = (u, v)$, the adversary asks the decryption oracle to decrypt the message $(u, 2v \bmod p)$. The received plaintext will either be $2M_0$ or $2M_1$ and will allow the adversary to allways win the game.