1 Nonce Reuse

In the ElGamal digital signature scheme, why should the same random nonce never be reused for 2 different messages with the same public/secret keypair?

2 Cryptographic Hash Functions

Let $h_1, h_2 : \{0, 1\}^* \rightarrow \{0, 1\}^n$ be two collision resistant functions. Are the following hash functions also collision resistant? Explain.

- $h_3(x) = h_1(x) \oplus h_2(x)$
- $h_4(x) = x_0 \cdot h_1(x)$

*Hint:* Try to find a collision or reduce the collision-resistance of the constructed hash functions to collision-resistance of $h_1$ and $h_2$.

3 IND-CPA

Let $h : \{0, 1\}^* \rightarrow \{0, 1\}^n$ be a collision resistant hash function, and let (Generate, Encrypt, Decrypt) be a correct and IND-CPA secure PK encryption scheme, as defined in the lecture. We define another PK encryption scheme (Generate’, Encrypt’, Decrypt’) as follows:

- Generate’() = Generate() = $(k_p, k_s)$ → *that is, the keys are generated in the same way*
- Encrypt’$(m, k_p) = (c_1, c_2) = (h(m), Encrypt(m, k_p))$ → *In other words, $h(m)$ is appended to the encrypted message.*
- Decrypt’$(c_1, c_2), k_s = Decrypt(c_2, k_s)$

* a) Show that the new scheme is a correct encryption scheme. That is, show that for any $m$ Decrypt’$(Encrypt’(m, k_p), k_s) = m$.

* b) Show that (Generate’, Encrypt’, Decrypt’) is not IND-CPA secure.

*Hint:* Think about the IND-CPA game and how can the adversary win with non-negligible probability.

\[x_0 \text{ means the first bit of the message } x, \text{ and as in the lecture, concatenation of messages is denoted by ;}\]