



Given a fixed message m_1 , if we cannot find in a practical way a different message m_2 such that $\text{hash}(m_2) = \text{hash}(m_1)$, then we say that this hash function is collision-resistant.

- In the digital signature scheme, why do we produce the signature on the hash of the document and not on the document directly?
- Why is it important that hash functions are collision-resistant?

Exercise 3: (Caesar)

Break the following ciphertext, given that the Caesar cipher was used to produce it:

YVTL DHZ UVA IBPSA PU H KHF

(Hint: Start by a permutation of the alphabet by 1, then 2, ... until the result makes sense in English)

Exercise 4: (Misc)

- Describe differences between symmetric and asymmetric cryptosystems.
- Why is certification of public keys necessary? Name an attack that is possible if keys are not certified.