Asymmetric Cryptography Overview

Marcio Woitek

Problem 1

- $\mathrm{Dec}(k_1, \mathrm{Enc}(K_1, p)) = p$
- $\mathrm{Dec}(K_2, \mathrm{Enc}(k_2, p)) = p$

Problem 2

- Key distribution and management should be addressed when using asymmetric cryptography.

Problem 3

- Both the public key and the private key should remain secret against an attacker.
- Both the sender and the receiver can use the same private key for encryption and decryption.

Problem 4

- Solving $f(x)$ if the input and k are known.
- Solving the inverse of f if the input to the f-inverse and k are known.

Problem 5

- Encryption/decryption
- Key exchange
- Digital signature

Problem 6

- Key exchange