Public Key Cryptography

Federico Casu

December 21, 2023

Public Key Cryptography: a brief introduction

As we are becoming familiar with it, let's study how *public key cryptography* is used to protect communications. Figure 1 illustrates the fundamentals of a public key-based communication system:

- Alice, who wants to send a confidential message to Bob, knows Bob's public key $\mathsf{K}_{\mathsf{pub}}^{(\mathsf{B})}$. To encrypt the message x, Alice executes the encryption algorithm $\mathsf{E}(\cdot)$, taking as input the plaintext x and Bob's public key $\mathsf{K}_{\mathsf{pub}}^{(\mathsf{B})}$.
- Bob, who wants to read the incoming message (and correctly decrypt y), executes the decryption algorithm $\mathsf{E}^{-1}(\cdot)$, taking as input the ciphertext y and Bob's private key $\mathsf{K}_{\mathsf{priv}}^{(\mathsf{B})}$.

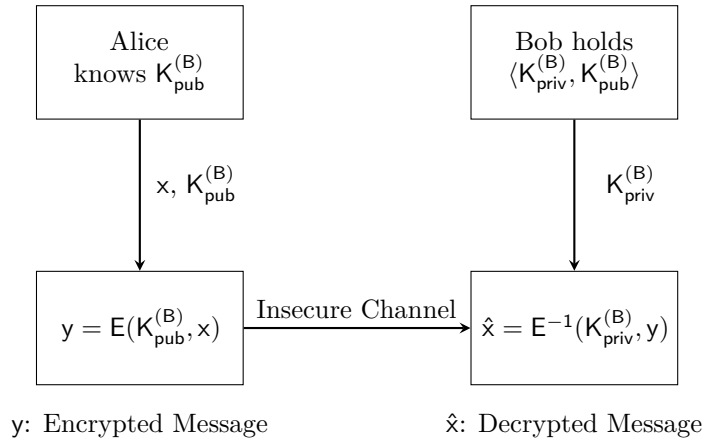

Figure 1: Public Key Cryptography - Simple communication scenario.