

Cryptographic tasks for honest participants

Paul Dumais, November 2002

Conventional Cryptography

public subroutines: $\text{encr}()$, $\text{decr}()$

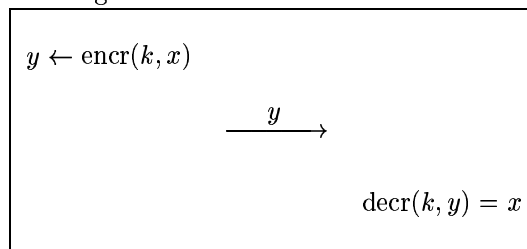
Alice

secret key: k

message: x

Bob

secret key: k



Public Key Cryptography

public subroutines: $\text{encr}()$, $\text{decr}()$

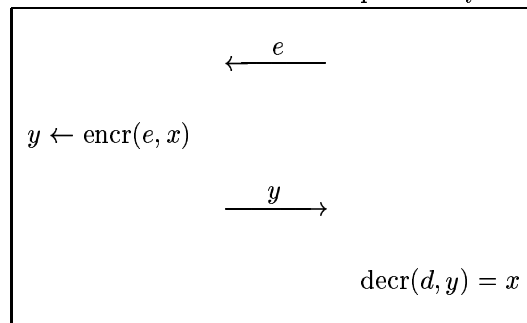
Alice

message: x

Bob

secret key: d

public key: e



Message Authentication

public subroutine: $\text{hash}()$

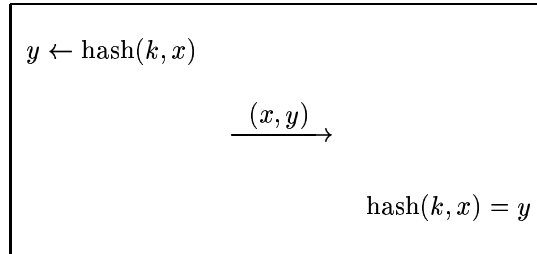
Alice

secret key: k

message: x

Bob

secret key: k



Digital Signature

public subroutines: $\text{sign}()$, $\text{verif}()$

Alice

secret key: k

public key: l

message: x

Bob

