Cryptography

Public Key Encryption

KA-security

$(T, k) \leftarrow \text{EXEC}(\Pi)$

$L^{\Pi}_{ka-real}$
QUERY():
$(T, k) \leftarrow \text{EXEC}(\Pi)$
return (T, k)

$L^{\Pi}_{ka-rand}$
QUERY():
$(T, k) \leftarrow \text{EXEC}(\Pi)$
$r \leftarrow \Pi.K$
return (T, r)

Problems and Assumptions in DL-Type in Cryptography

DLP (Discrete Logarithm Problem

Given: $\langle g \rangle = G, \mid G \mid = q$