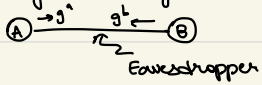
Diffie-Hellman

Secret Key Establishment

Assume: DLP is hard in cyclic group G with generator g



Protocol:

① A chooses a $\in_R [1, \ldots |G|]$ & computes g^a. $\forall Z_p^*$, a $\in_R [1, \ldots p-1]$, $g^a \bmod p$

② B choose b $\in_R [1, \ldots |G|]$ & computes g^b.

③ Exchange g^a & g^b

④ $K_A = (g^b)^a$, $K_B = (g^a)^b$ } equal

Correctness ☑

Security: Eavesdropper cannot get a & b from g^a & g^b since DLP is hard. DLP being hard is a necessary but maybe sufficient assumption since Env might get g^{ab} without finding a & b.

Necessary + Sufficient: DDH Assumption

(Intuitively, given g^a & g^b, g^{ab} is hard to get)

$\forall$ PPTM A, $\left| P(A(g^a, g^b, r) = 1) - P(A(g^a, g^b, g^{ab}) = 1) \right| \leq \text{negl}(\log |G|)$

r random

CDH Assumption: No efficient way to get g^{ab} from g^a & g^b

CDH - Computation Diffie Hellman Assumption

DDH - Decisional " " "

Integer factorization

Computational: Calculate factors with high probability

Decisional: Are there factors

Instead $\{ \langle N, l, u \rangle \mid \exists d | N, l \leq d \leq u \}$

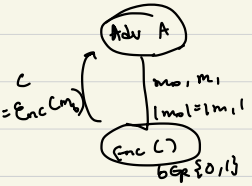
$Gen(1^n)$: $\langle S_k, P_k \rangle$

$Enc_{P_k}(m) = C$

$Dec_{S_k}(c) = m$

There cannot be a perfectly secure public key cryptography system.

$\langle Gen, Enc, Dec \rangle$ is CPA secure if



No need Enc server since public key is available

$\forall$ PPTM A,

$Pr[A(P_k, c) = b] \leq \frac{1}{2} + \text{negl}(n)$

RSA is deterministic, so internet uses Padded RSA, but RSA-OAEP is provably CPA secure.

El-Gamal Public Key Encryption:

Let Cyclic group G on which DLP is hard

$P_k = \langle G, g, q = |G|, g^a \rangle$

$Enc_{P_k}(m) = \langle g^b, g^{ab} \cdot m \rangle \cdot \langle u, v \rangle$

$b \in_R G$

$Dec_{S_k}(m) = \frac{v}{u^{S_k}}$

$S_k = \langle a \rangle$

$\gcd(a, p) = 1 \Rightarrow xa + yp = 1$

$x \bmod p = a^{-1}$