Cryptology 19th November, 2015

Lecture 14: Key Exchange Protocols

Instructor: Dr. Goutam Paul *Scribe: Mayank Raikwar*

1 Key Exchange Protocol

Key exchange is any method in cryptography by which cryptographic keys are exchanged between two parties, allowing use of a cryptographic algorithm.

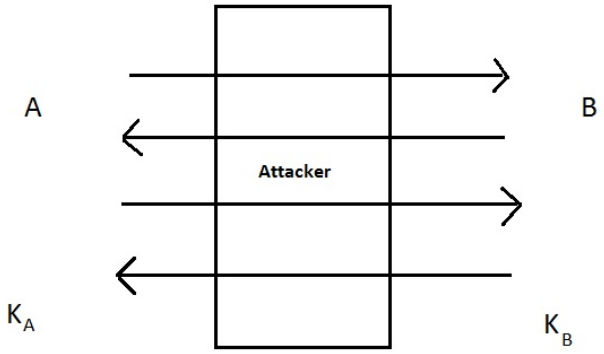

Figure 1: Key Exchange

Correctness : $K_A = K_B$
Security :

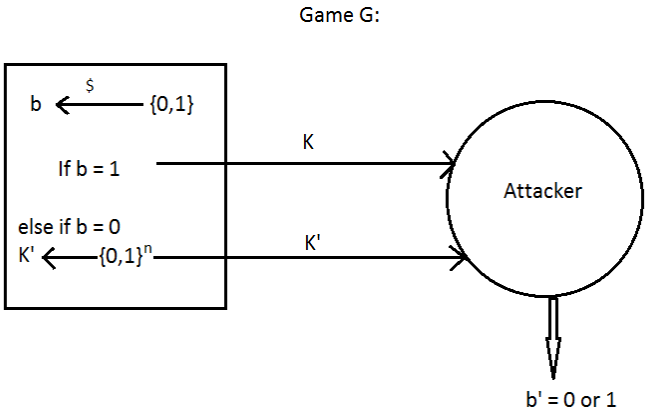

Figure 2: Game between challanger and attacker

• n : Length of K in bits
• Attacker A wins the game if $b = b'$
• Protocol π is a secure key exchange protocol iff

$$Pr[A \text{ wins } G] \leq \tfrac{1}{2} + \text{negl}(n)$$

Here negl(n) is advantage.
Example : **Diffie-Hellman Key Exchange protocol**

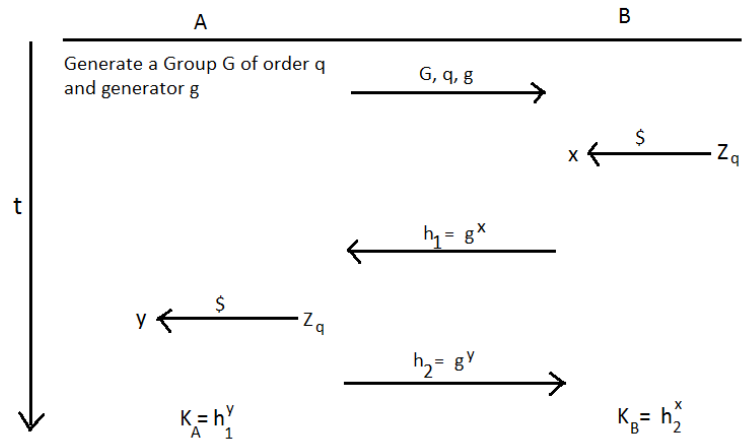

Figure 3: Diffie-Hellman Key Exchange

Correctness :

$$\left.\begin{array}{l} K_A = {h_1}^y = (g^x)^y = g^{xy} \\ K_B = {h_1}^y = (g^x)^y = g^{xy} \end{array}\right\} K_A = K_B$$

Security :Attacker knows $G, q, g, h_1 = g^x$ and $h_2 = g^y$. Can he/she determine $K = K_A = K_B = g^{xy}$?

Assumptions :
•Discrete Log problem assumption(DLP)⇒ Given g, g^x, it is hard to compute x.
•Computational DiffieHellman assumption(CDH)⇒ Given g, g^x, g^y it is hard to compute g^{xy}.
•Decisional DiffieHellman assumption(DDH)⇒ It is hard to distinguish (g, g^x, g^y, g^{xy}) and (g, g^x, g^y, g^z) where $z \overset{\$}{\leftarrow} Z_q$

Here DLP is at least as hard as CDH and CDH is at least as hard as DDH.Thus DDH is sufficient condition while CDH and DLP are necessary conditions.

$\Rightarrow$ **Pr[A wins the distinguishing game G]**
$= Pr[b' = b]$
$= Pr[b = 0 \cap b' = 0] + Pr[b = 1 \cap b' = 1]$
$= Pr[b = 0]Pr[b' = 0|b = 0] + Pr[b = 1]Pr[b' = 1|b = 1]$
$= \frac{1}{2}Pr[A(g, g^x, g^y, g^r) = 0] + \frac{1}{2}Pr[A(g, g^x, g^y, g^{xy}) = 1]$
$= \frac{1}{2}[1 - Pr[A(g, g^x, g^y, g^r) = 1]] + \frac{1}{2}Pr[A(g, g^x, g^y, g^{xy}) = 1]$
$= \frac{1}{2} + \frac{1}{2}[Pr[A(g, g^x, g^y, g^{xy}) = 1] - Pr[A(g, g^x, g^y, g^r) = 1]]$
$\leq \frac{1}{2} + \frac{1}{2}.\epsilon$
$\leq \frac{1}{2}+$ negl(n) here ϵ is negl(n) by DDH assumption.

1.1 Attack

Man-in-the-middle attack:It is an attack where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other.

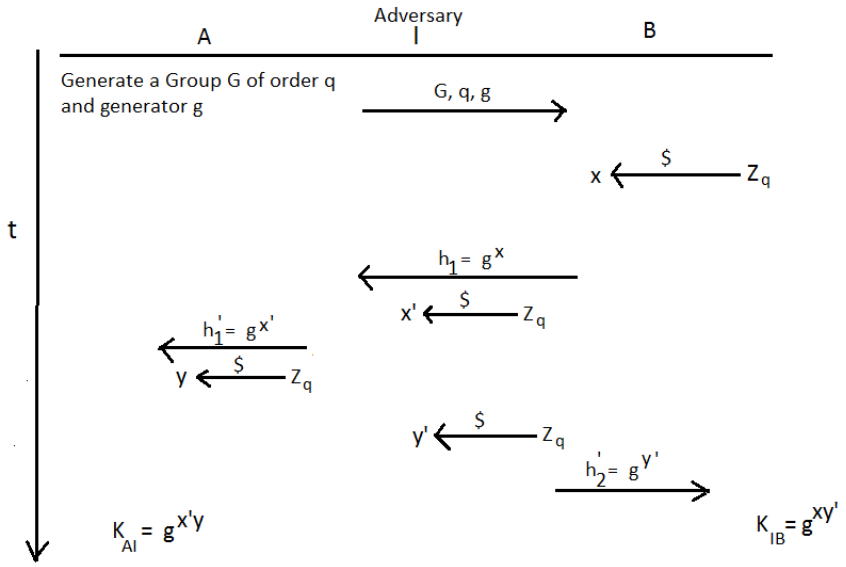

Figure 4: Man-in-the-middle attack

Fixing MIM attack: Authenticated Key Exchange(AKE)