Man in the Middle Attack on the Analog of Massey Omura over Elliptic Curves

Abstract

The man in the middle attack on the analog of Massey Omura over Elliptic curves may look confusing but is trivial and is as discussed.

Introduction

Let Alice and Bob be two legitimate users attempting secure communication over an insecure channel and Mallory be the man in the middle.

Let e*d== 1 mod N
N,the order of the curve is public.

Let
e_A=public key for Alice
d_A=private key of Alice

e_M=public key for Mallory
d_M=private key of Mallory

e_B=public key for Bob
d_B=private key of Bob

Let P be the secret embedded on the elliptic curve. Since the point P has to be a point on the elliptic curve, we cannot choose all the bits of P to hold the secret. There are a few don't care bits using which it is feasible to determine P such that it lies on the elliptic curve.

The Attack

Alice $\longleftrightarrow$ Mallory $\longleftrightarrow$ Bob

1.Alice ($P.e_A$) $\longrightarrow$ Mallory($P.e_A$)

Alice computes $P.e_A$ and sends it to Bob which is intercepted by Mallory.

2.Alice ($P.e_A.e_M$) $\longleftarrow$ Mallory ($P.e_A.e_M$)

Mallory then computes $P.e_A.e_M$ and then sends it to Alice.

3.Alice ($P.e_A.d_A.e_M=P.e_M$) $\longrightarrow$ Mallory ($P.e_M$; $P.d_M.e_M=P$)

Alice computes $P.e_M$ and is intercepted by Mallory. Mallory computes $P.d_M.e_M=P$. The secret is out. Now,we deal with Bob.

4.Mallory ($P.e_M$) $\longrightarrow$ Bob($P.e_M$; $P.e_M.e_B$)

Mallory computes $P.e_M$ and sends it to Bob. Bob computes $P.e_M.e_B$

5.Mallory ($P.e_M.e_B$) $\longleftarrow$ Bob($P.e_M.e_B$)

Bob sends $P.e_M.e_B$ and is intercepted by Mallory.

6.Mallory($P.e_M.d_M.e_B=P.e_B$) $\longrightarrow$ Bob($P.e_B$; $P.e_B.d_B=P$)

Mallory computes $P.e_B$ and sends it to Bob. Bob computes $P.e_B.d_B=P$. This completes the man in the middle attack.

-By Sarad A.V