Diffie Helman

Author(s): W. Diffie and M. Helman 1978
Last modified November 11, 2002

Summary: The Diffie Helman key exchange algorithm.

Protocol specification (in common syntax)

```
A, B :          principal
P, G, Xa, Xb :  number
one :            -> number
kap :           number, number, number -> number
```

```
1.    A  ->  B  :    P, G
2.    A  ->  B  :    kap(P, G, Xa)
3.    B  ->  A  :    kap(P, G, Xb)
4.    A  ->  B  :    {one()}kap(P, kap(P, G, Xb), Xa)
```

Description of the protocol rules

The function `kap` must satisfy:

$$\texttt{kap(P, kap(P, G, Y), X)} = \texttt{kap(P, kap(P, G, X), Y)}$$

It is implemented by: `kap(P, X, Y) = exp(X, Y) mod P`.

It the protocol, `P` is choosen to be a prime number `P` and `G < P`.

The fresh symmetric key exchanged is `kap(P,kap(P,G,Xb),Xa)` = `kap(P,kap(P,G,Xa),Xb)`.

Requirements

The protocol must guaranty the secrecy of the fresh key.

The protocol must guaranty the authenticity of the participants.

References

[DH76]

Claimed proofs

[Bla01]

Claimed attacks

The authenticity is not guaranteed by the protocol.

```
1.    I(A)  ->    B    :    P, G
2.    I(A)  ->    B    :    kap(P, G, Xi)
3.      B   ->  I(A)   :    kap(P, G, Xb)
4.    I(A)  ->    B    :    {one()}kap(P, kap(P, G, Xb), Xi)
```

or

```
1.      A   ->  I(B)   :    P, G
2.      A   ->  I(B)   :    kap(P, G, Xa)
3.    I(B)  ->    A    :    kap(P, G, Xi)
4.      A   ->  I(B)   :    {one()}kap(P, kap(P, G, Xi), Xa)
```

Citations

[Bla01] Bruno Blanchet. An efficient cryptographic protocol verifier based on prolog rules. In IEEE, editor, *14th IEEE Computer Security Foundations Workshop (CSFW-14)*, june 2001.

[DH76] W. Diffie and M. Helman. New directions in cryptography. *IEEE Transactions on Information Society*, 22(6):644–654, november 1976.