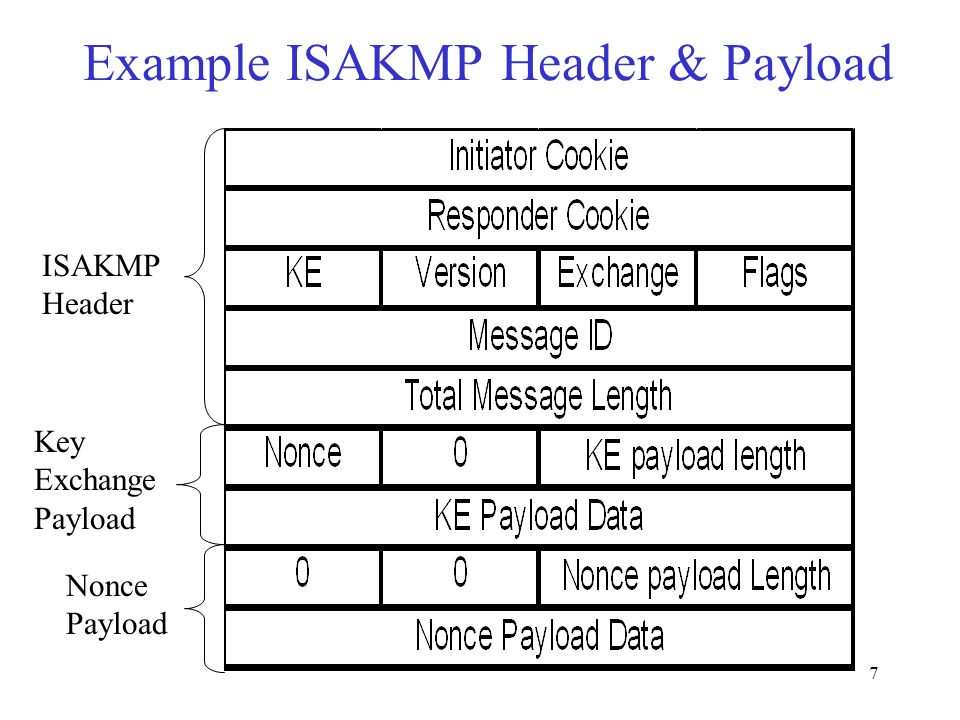
IKE phase 1( RFC 4306 ,RFC 5996, RFC 7296 and RFC 7427

Handshake

Authentication <- certification/pre-shared key

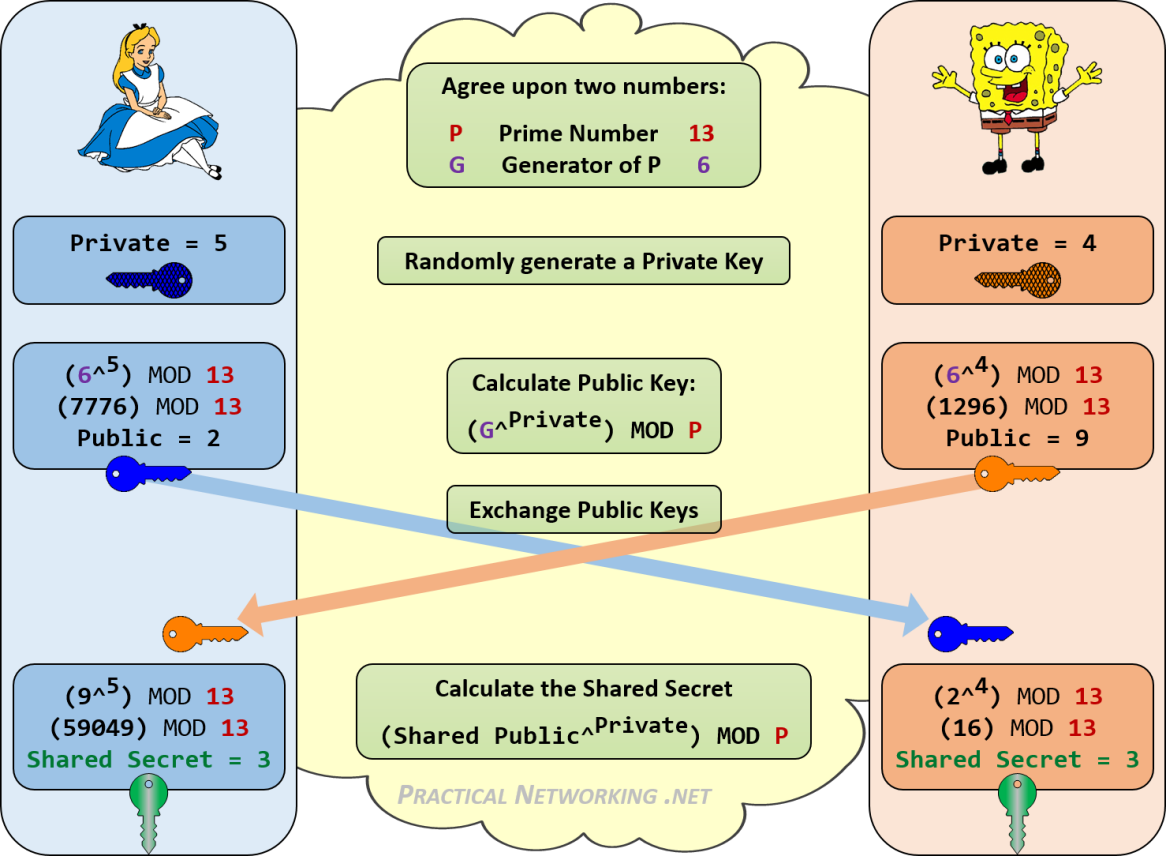
**Diffie**-**Hellman(MODP group) -> SA**



**IKE phase 2**

**ESP tunnel**

**Diffie-Hellman:**



**RFC3526: MODP group 14(2048 bits)**

## **2048-bit MODP Group**

This group is assigned id 14.

This prime is: 2^2048 - 2^1984 - 1 + 2^64 \* { [2^1918 pi] + 124476 }

Its hexadecimal value is:

FFFFFFFF FFFFFFFF C90FDAA2 2168C234 C4C6628B 80DC1CD1

29024E08 8A67CC74 020BBEA6 3B139B22 514A0879 8E3404DD

EF9519B3 CD3A431B 302B0A6D F25F1437 4FE1356D 6D51C245

E485B576 625E7EC6 F44C42E9 A637ED6B 0BFF5CB6 F406B7ED

EE386BFB 5A899FA5 AE9F2411 7C4B1FE6 49286651 ECE45B3D

C2007CB8 A163BF05 98DA4836 1C55D39A 69163FA8 FD24CF5F

83655D23 DCA3AD96 1C62F356 208552BB 9ED52907 7096966D

670C354E 4ABC9804 F1746C08 CA18217C 32905E46 2E36CE3B

E39E772C 180E8603 9B2783A2 EC07A28F B5C55DF0 6F4C52C9

DE2BCBF6 95581718 3995497C EA956AE5 15D22618 98FA0510

15728E5A 8AACAA68 FFFFFFFF FFFFFFFF

The generator is: 2.

**References**

1. **<https://www.practicalnetworking.net/series/cryptography/diffie-hellman/>**
2. **<https://tools.ietf.org/html/rfc3526>**