

Diffie-Hellman-Merkle in practice

- g is small (either 3, 5 or 7 and fixed in practice)
 - p is at least 2048 bits (and fixed in practice)
 - private keys a and b are 2048 bits as well
- ➔ So the public values A and B
and the master key k are 2048 bits
- ➔ Use k to derive an AES key using a Key Derivation Function
(usually HKDF - the HMAC-based Extract-and-Expand key derivation function)

Elliptic Curve Diffie-Hellman-Merkle (ECDH)

- ➔ Generate a symmetric key k from two distinct asymmetric key pairs: K_{pA}, K_{sA} and K_{pB}, K_{sB}

$$k = \text{ECDH}(K_{sA}, K_{pB}) = \text{ECDH}(K_{sB}, K_{pA})$$