**Cryptographic technique – 2(Deffie Hellman key exchange)**

Deffie-Hellman cryptographic technique is an asymmetric technique which includes both public and private keys. This method includes exchanging of cryptographic keys over a public channel securely. The technique is illustrated with an example below:

1. There are two people: Alice and Bob who need to exchange their keys. Both agree to use modulus p = 23 and g = 5.
2. Alice chooses a secret integer *a* = 6, then sends Bob *A* = *ga* mod *p*
   1. *A* = 56 mod 23 = 8
3. Bob chooses a secret integer *b* = 15, then sends Alice *B* = *gb* mod *p*
   1. *B* = 515 mod 23 = 19
4. Alice computes *s* = *Ba* mod *p*
   1. *s* = 196 mod 23 = 2
5. Bob computes *s* = *Ab* mod *p*
   1. *s* = 815 mod 23 = 2
6. Alice and Bob now share a secret (the number 2).

Thus, exchanging of secret keys is securely possible which can be then used to encrypt and decrypt a message to be sent.

**References:**

<https://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange>

https://community.jisc.ac.uk/library/advisory-services/introduction-cryptographic-techniques