NAME

DH_generate_key, DH_compute_key - perform Diffie-Hellman key exchange

SYNOPSIS

```
#include <openssl/dh.h>

int DH_generate_key(DH *dh);

int DH_compute_key(unsigned char *key, BIGNUM *pub_key, DH *dh);
```

DESCRIPTION

DH_generate_key() performs the first step of a Diffie-Hellman key exchange by generating private and public DH values. By calling *DH_compute_key()*, these are combined with the other party's public value to compute the shared key.

DH_generate_key() expects **dh** to contain the shared parameters **dh->p** and **dh->g**. It generates a random private DH value unless **dh->priv_key** is already set, and computes the corresponding public value **dh->pub_key**, which can then be published.

DH_compute_key() computes the shared secret from the private DH value in **dh** and the other party's public value in **pub_key** and stores it in **key**. **key** must point to **DH_size(dh)** bytes of memory.

RETURN VALUES

DH_generate_key() returns 1 on success, 0 otherwise.

DH_compute_key() returns the size of the shared secret on success, -1 on error.

The error codes can be obtained by *ERR_get_error(3)*.

SEE ALSO

dh(3), *ERR_get_error(3)*, *rand(3)*, *DH_size(3)*

HISTORY

DH_generate_key() and *DH_compute_key()* are available in all versions of SSLeay and OpenSSL.