NAME

dh - Diffie-Hellman key agreement

SYNOPSIS

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

DH * DH_new(void);
void DH_free(DH *dh);

int DH_size(const DH *dh);

DH * DH_generate_parameters(int prime_len, int generator,
void (*callback)(int, int, void *), void *cb_arg);
int DH_check(const DH *dh, int *codes);

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

void DH_set_default_method(const DH_METHOD *meth);
const DH_METHOD *DH_get_default_method(void);
int DH_set_method(DH *dh, const DH_METHOD *meth);
DH *DH_new_method(ENGINE *engine);
const DH_METHOD *DH_OpenSSL(void);

int DH_get_ex_new_index(long argl, char *argp, int (*new_func)(),
int (*dup_func)(), void (*free_func)());
int DH_set_ex_data(DH *d, int idx, char *arg);
char *DH_get_ex_data(DH *d, int idx);

DH * d2i_DHparams(DH **a, unsigned char **pp, long length);
int i2d_DHparams(const DH *a, unsigned char **pp);

int DHparams_print_fp(FILE *fp, const DH *x);
int DHparams_print(BIO *bp, const DH *x);
```

DESCRIPTION

These functions implement the Diffie-Hellman key agreement protocol. The generation of shared DH parameters is described in *DH_generate_parameters(3)*; *DH_generate_key(3)* describes how to perform a key agreement.

The **DH** structure consists of several BIGNUM components.

```
struct
{
BIGNUM *p; // prime number (shared)
BIGNUM *g; // generator of Z_p (shared)
BIGNUM *priv_key; // private DH value x
BIGNUM *pub_key; // public DH value gx
// ...
};
DH
```

Note that DH keys may use non-standard **DH_METHOD** implementations, either directly or by the use of **ENGINE** modules. In some cases (eg. an ENGINE providing support for hardware-embedded keys), these BIGNUM values will not be used by the implementation or may be used for alternative data storage. For this reason, applications should generally avoid using DH structure

elements directly and instead use API functions to query or modify keys.

SEE ALSO

dhparam(1), *bn(3)*, *dsa(3)*, *err(3)*, *rand(3)*, *rsa(3)*, *engine(3)*, *DH_set_method(3)*, *DH_new(3)*, *DH_get_ex_new_index(3)*, *DH_generate_parameters(3)*, *DH_compute_key(3)*, *d2i_DHparams(3)*, *RSA_print(3)*