Генерирование пары ключей

```
openssl genpkey [-help][-out filename][-outform DER|PEM][-verbose][-quiet]
[-pass arg][-cipher][-paramfile file][-algorithm alg][-pkeyopt opt:value]
[-genparam][-text][-engine id][-provider name][-provider-path path]
[-propquery propq][-config configfile]
```

-pkeyopt *opt:value*
: Устанавливает значение параметра алгоритма открытого ключа *opt* равным *value*. Точный набор поддерживаемых опций зависит от используемого алгоритма открытого ключа и его реализации.

  Получить дополнительную информацию о возможных значениях opt в зависимости от алгоритма, описании остальных опций

-algorithm *alg*
: Алгоритм публичного ключа. Если используется, должно предшествовать опции -pkeyopt. -paramfile и -algorithm взаимоисключают друг друга.

  Встроенные алгоритмы генерации публичного ключа: RSA, RSA-PSS, EC, X25519, X448, ED25519 и ED448.

  Встроенные алгоритмы генерации параметров: DH, DSA и EC.

-out *filename*
: Вывести ключ в указанный в *filename* файл. Если этот аргумент не указан, используется стандартный вывод.

Генерация пары ключей EC:

```
openssl genpkey ^
      -algorithm EC ^
      -pkeyout ec_paramgen_curve:secp521r1 ^
      -out ec_keypair.pem
```

Просмотр структуры ключей, извлечение открытого ключа из пары

```
openssl pkey [-help][-inform PEM|DER][-outform PEM|DER][-in filename]
[-passin arg][-out filename][-passout arg][-traditional][-cipher][-text]
[-text_pub][-noout][-pubin][-pubout][-engine id][-check][-pubcheck]
```

-in *filename*
: Здесь указывается имя входного файла для чтения ключа или стандартный ввод, если этот параметр не указан. Если ключ зашифрован, будет запрошен пароль.

-noout
: Не выводить закодированную версию ключа.

-text
: Выводит различные компоненты открытого или закрытого ключа в виде обычного текста в дополнение к закодированной версии.

-pubin
: По умолчанию закрытый ключ считывается из входного файла: при использовании этой опции вместо этого считывается открытый ключ.

-pubout
: По умолчанию выводится закрытый ключ: при использовании этой опции вместо него будет выводиться открытый ключ. Этот параметр устанавливается автоматически, если входные данные являются открытым ключом.

-out *filename*
Здесь указывается имя выходного файла, в который нужно записать ключ, или стандартный вывод, если эта опция не указана. Если установлены какие-либо параметры шифрования, будет запрошен пароль. Имя выходного файла НЕ должно совпадать с именем входного файла.

Получить дополнительное описание опций

Просмотр структуры пары ключей EC:
```
openssl pkey -in ec_keypair.pem -noout -text
```

Извлечение открытого ключа из пары ключей EC:
```
openssl pkey ^
      -in ec_keypair.pem ^
      -pubout ^
      -out ec_public_key.pem
```

Подписание и проверка подписи в командной строке

```
openssl pkeyutl [-help][-in file][-out file][-sigfile file][-inkey file]
[-keyform PEM|DER|ENGINE][-passin arg][-peerkey file][-peerform PEM|DER|ENGINE]
[-pubin][-certin][-rev][-sign][-verify][-verifyrecover][-encrypt][-decrypt]
[-kdf algorithm][-kdflen length][-pkeyopt opt:value][-hexdump][-asn1parse]
[-rand  file][-writerand file][-engine id][-engine_impl]
```

-sign
Подписать входные данные (которые должны быть хешем) и вывести подписанный результат. Для этого требуется закрытый ключ.

-inkey *file*
Входной файл ключа, по умолчанию это должен быть закрытый ключ.

-in *file*
Здесь указывается имя входного файла для чтения данных или стандартный ввод, если эта опция не указана.

-out *file*
Здесь указывается имя выходного файла для записи или стандартный вывод по умолчанию.

-verify
Проверяет входные данные (которые должны быть хешем) по файлу подписи и указывает прошла ли проверка успешно или нет.

-sigfile *file*
Файл подписи, требуется только для операции проверки verify.

Подписание файла, используя функцию хеширования SHA3-512 и ранее сгенерированную пару ключей EC:
```
openssl pkeyutl ^
      -sign ^
      -digest sha3-512 ^
      -inkey ec_keypair.pem ^
      -in somefile.txt ^
      -rawin ^
      -out somefile.txt.signature
```

Проверка подписи:
```
openssl pkeyutl ^
      -verify ^
      -digest sha3-512 ^
      -inkey ec_keypair.pem ^
      -in somefile.txt ^
      -rawin ^
      -sigfile somefile.txt.signature
```