34.11-2012

34.11-2012. /etc/shadow. :

```
$<__>$<_>$<_>
```

:

- __ — gost12512hash;
- _ — , () (, salt). saltsaltsaltsalt;
- _ — , .

"$" (). :

```
$gost12512hash$saltsaltsaltsalt$Y.AHSfY6w10hNisNhRQkl3YuAexXkTWxDAI2sipxMVG.
wVHgZ5czD2wX2zMpptQEu2Wpfuo7DiAKDxDWe/IjS0
```

gost12_512_crypt() libgost. libgost Astra Linux . , libgost.so /lib/libgost.so.2.0.2 (Astra Linux x.7, 1.6.12, 2.12.46). , :

```
dpkg -L libgost
```

34.11-2012 gost12_512_crypt()

gcc (gcc). gcc ALSE x.7 , Astra Linux Special Edition . :

```
sudo apt install gcc
```

-2012-512 gost12_512_crypt()

:

```
#include <stdio.h>

//    .
//   - ,   -
extern char *gost12_512_crypt (const char *pass, const char *salt); //    . 1-

const char *pass = "q2w2e2r2";         //
const char *salt = "saltsaltsaltsalt"; // ""

int main( int argc, char **argv) {
        char *hash = gost12_512_crypt( pass, salt);
        if( !hash) {
                fprintf( stderr, "Failed %m\n");
                return 1;
        }
        printf( "pass=%s salt=%s hash=%s\n", pass, salt, hash);
        return 0;
}
```

(, hach.c):

```
gcc hash.c /lib/libgost.so.2.0.2
```

 a.out. :

```
./a.out
salt=q2w2e2r2 pass=saltsaltsaltsalt hash=$gost12512hash$saltsaltsaltsalt$Y.
AHSfY6w10hNisNhRQkl3YuAexXkTWxDAI2sipxMVG.wVHgZ5czD2wX2zMpptQEu2Wpfuo7DiAKDxDWe/IjS0
```

-2012-512 gost12_512_crypt() Python

 -2012-512 gost12_512_crypt() Python .

:

```
#!/usr/bin/python3

import base64, ctypes, getpass, os, sys

def gost12_512_crypt(key, salt):
    libgost = ctypes.cdll.LoadLibrary("/lib/libgost.so.2.0.2")

    libgost.gost12_512_crypt.argtypes = (
        ctypes.c_char_p,
        ctypes.c_char_p,
    )
    libgost.gost12_512_crypt.restype = ctypes.c_void_p

    c_void_ptr = libgost.gost12_512_crypt(key.encode(), salt.encode())
    c_result = ctypes.cast(c_void_ptr, ctypes.c_char_p)

    return c_result.value.decode()

if __name__ == "__main__":
    salt = (
        sys.argv[1]
        if len(sys.argv) > 1
        else base64.urlsafe_b64encode(os.urandom(12)).decode("ascii").rstrip("=")
    )
    print(gost12_512_crypt(getpass.getpass(), salt))
```

, hash.py. "" (-). , . :

```
python3 hash.py saltsaltsaltsalt
Password:
$gost12512hash$saltsaltsaltsalt$Y.AHSfY6w10hNisNhRQkl3YuAexXkTWxDAI2sipxMVG.
wVHgZ5czD2wX2zMpptQEu2Wpfuo7DiAKDxDWe/IjS0
```