

Шифруем файлы при помощи age и публичных ключей

Если у вас есть публичный ключ получателя в формате id_ed25519 (Ed25519), то для шифрования файлов лучше использовать age — современный, простой и безопасный инструмент. Ed25519 напрямую не поддерживается OpenSSL для шифрования, но age отлично работает с такими ключами.

Установка age

Ubuntu/Debian

```
sudo apt-get install age
```

macOS

```
brew install age
```

Windows (choco)

```
choco install age
```

Или скачайте бинарный файл с GitHub: <https://github.com/FiloSottile/age/releases>

Шифрование/Расшифровка файла ключом Ed25519

Зашифровать исходный файл secret.txt

```
age -R id_ed25519.pub -o secret.txt.age secret.txt
```

Расшифровка файла приватным ключом зашифрованный файл secret.txt.age

```
age -d -i ~/.ssh/id_ed25519 -o decrypted.txt secret.txt.age
```

Публичный ключ из файла id_ed25519.pub

```
age -r "ssh-ed25519 AAAA..." -o file.txt.age file.txt
```

Или если ключ в файле

```
age -R ~/.ssh/id_ed25519.pub -o file.txt.age file.txt
```

Извлечь публичный ключ в нужном формате (если нужно)

```
ssh-keygen -y -f ~/.ssh/id_ed25519 > id_ed25519.pub
```

[шифрование файлов](#), [encrypt files](#), [age](#), [id ed25519](#)

From:

<https://wiki.rtzra.ru/> - **RTzRa's hive**

Permanent link:

<https://wiki.rtzra.ru/software/crypt-files-with-age>

Last update: **2026/02/02 21:26**

