

# Шифрование

## Алгоритм обмена Диффи-Хеллмана (DH)

Алгоритм обмена Диффи-Хеллмана (DH) — это метод, по которому две (а в некоторых случаях и более) сторон могут независимо создать один и тот же общий секрет, который затем может использоваться в симметричных криптографических алгоритмах (в TLS, например, DH используется для создания ключа, применяемого в фазе протокола записи данных). Предполагается, что весь сеанс, в течение которого происходит коммуникация двух сторон, может быть перехвачен третьей стороной. Эта третья сторона не сможет вывести тот же самый ключ, поскольку для этого ей не будет хватать некоторой информации.

## Ссылки

[Воп BOS: Безопасность \(Сертификаты\)](#)

[Pro-LDAP.ru - Руководство по выживанию — шифрование, аутентификация, отпечатки, MAC и подписи](#)

[Pro-LDAP.ru - Руководство по выживанию — TLS/SSL и сертификаты SSL \(X.509\), подписанные УЦ и самоподписанные](#)

[pic.ru — Я занимаюсь бизнесом и совсем не понимаю, что такое SSL-сертификаты](#)

<https://wiki.yola.ru/encryption/encryption>

2020-03-27 22:48

