**Криптография** — наука о методах обеспечения [конфиденциальности](https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BD%D1%84%D0%B8%D0%B4%D0%B5%D0%BD%D1%86%D0%B8%D0%B0%D0%BB%D1%8C%D0%BD%D0%BE%D1%81%D1%82%D1%8C) (невозможности прочтения информации посторонним), [целостности данных](https://ru.wikipedia.org/wiki/%D0%A6%D0%B5%D0%BB%D0%BE%D1%81%D1%82%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%B8)(невозможности незаметного изменения информации), [аутентификации](https://ru.wikipedia.org/wiki/%D0%90%D1%83%D1%82%D0%B5%D0%BD%D1%82%D0%B8%D1%84%D0%B8%D0%BA%D0%B0%D1%86%D0%B8%D1%8F) (проверки подлинности авторства или иных свойств объекта), а также невозможности отказа от авторства.

Изначально криптография изучала методы шифрования информации — обратимого преобразования открытого (исходного) текста на основе секретного алгоритма или [ключа](https://ru.wikipedia.org/wiki/%D0%9A%D0%BB%D1%8E%D1%87_(%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F)) в шифрованный текст (шифротекст).

Криптография не занимается защитой от обмана, подкупа или шантажа законных абонентов, кражи ключей и других [угроз](https://ru.wikipedia.org/wiki/%D0%A3%D0%B3%D1%80%D0%BE%D0%B7%D0%B0) информации, возникающих в защищённых системах передачи данных.

Криптография — одна из старейших наук, её [история](https://ru.wikipedia.org/wiki/%D0%98%D1%81%D1%82%D0%BE%D1%80%D0%B8%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D0%B8) насчитывает несколько тысяч лет.

Симметричный - способ шифрования, в котором для [шифрования](https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5) и [расшифровывания](https://ru.wikipedia.org/wiki/%D0%94%D0%B5%D1%88%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%BA%D0%B0) применяется один и тот же криптографический [ключ](https://ru.wikipedia.org/wiki/%D0%9A%D0%BB%D1%8E%D1%87_(%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F)).

Асимметричный - система [шифрования](https://ru.wikipedia.org/wiki/%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F) и/или [электронной подписи](https://ru.wikipedia.org/wiki/%D0%AD%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D1%86%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B0%D1%8F_%D0%BF%D0%BE%D0%B4%D0%BF%D0%B8%D1%81%D1%8C), при которой *открытый ключ* передаётся по открытому (то есть незащищённому, доступному для наблюдения) каналу и используется для шифрования сообщения. Для расшифровки сообщения используется [закрытый ключ](https://ru.wikipedia.org/wiki/%D0%97%D0%B0%D0%BA%D1%80%D1%8B%D1%82%D1%8B%D0%B9_%D0%BA%D0%BB%D1%8E%D1%87)[[1]](https://ru.wikipedia.org/wiki/%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0_%D1%81_%D0%BE%D1%82%D0%BA%D1%80%D1%8B%D1%82%D1%8B%D0%BC_%D0%BA%D0%BB%D1%8E%D1%87%D0%BE%D0%BC#cite_note-1).

\*\*\*Тимур – даун.\*\*\*

А также шифрование может использоваться в военных целях.

Машинка Enigma, использовавшаяся Германией в годы Второй мировой войны, была не уникальна. Но от аналогичных устройств, взятых на вооружение другими странами, она отличалась относительной простотой и массовостью использования: применить ее можно было практически везде — и в полевых условиях, и на подводной лодке. Работа ее заключалась в замене одних букв другими за счёт вращающихся валиков.

Enigma имела достаточно неплохое количество ключей для того времени - 15,896,255,521,782,636,000≈264­.