**Шифр Плейфера** или **квадрат Плейфера** — ручная [симметричная](https://ru.wikipedia.org/wiki/%D0%A1%D0%B8%D0%BC%D0%BC%D0%B5%D1%82%D1%80%D0%B8%D1%87%D0%BD%D0%BE%D0%B5_%D1%88%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5) техника [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), в которой впервые использована [замена биграмм](https://ru.wikipedia.org/wiki/%D0%91%D0%B8%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%BD%D1%8B%D0%B9_%D1%88%D0%B8%D1%84%D1%80). Изобретена в 1854 году английским [физиком](https://ru.wikipedia.org/wiki/%D0%A4%D0%B8%D0%B7%D0%B8%D0%BA) [Чарльзом Уитстоном](https://ru.wikipedia.org/wiki/%D0%A3%D0%B8%D1%82%D1%81%D1%82%D0%BE%D0%BD,_%D0%A7%D0%B0%D1%80%D0%BB%D1%8C%D0%B7), но названа именем [лорда](https://ru.wikipedia.org/wiki/%D0%9B%D0%BE%D1%80%D0%B4) [Лайона Плейфера](https://ru.wikipedia.org/w/index.php?title=%D0%9F%D0%BB%D0%B5%D0%B9%D1%84%D0%B5%D1%80,_%D0%9B%D0%B0%D0%B9%D0%BE%D0%BD,_1-%D0%B9_%D0%B1%D0%B0%D1%80%D0%BE%D0%BD_%D0%9F%D0%BB%D0%B5%D0%B9%D1%84%D0%B5%D1%80&action=edit&redlink=1)[[en]](https://en.wikipedia.org/wiki/Lyon_Playfair,_1st_Baron_Playfair), который внёс большой вклад в продвижение использования данной системы шифрования в государственной службе. Шифр предусматривает шифрование пар символов (биграмм) вместо одиночных символов, как в [шифре подстановки](https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80_%D0%BF%D0%BE%D0%B4%D1%81%D1%82%D0%B0%D0%BD%D0%BE%D0%B2%D0%BA%D0%B8) и в более сложных системах шифрования [Виженера](https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80_%D0%92%D0%B8%D0%B6%D0%B5%D0%BD%D0%B5%D1%80%D0%B0). Таким образом, шифр Плейфера более устойчив к взлому по сравнению с шифром простой замены, так как усложняется его частотный анализ. Он может быть проведён, но не для 26 возможных символов (латинский алфавит), а для 26 х 26 = 676 возможных биграмм, и значительно более трудоёмок и требует большего объёма зашифрованного текста.

Несмотря на то, что шифр был изобретением Уитстона, он стал известен как шифр Плейфера. Его первое описание было зарегистрировано в документе, подписанном Уитстоном 26 марта 1854 года[[1]](https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80_%D0%9F%D0%BB%D0%B5%D0%B9%D1%84%D0%B5%D1%80%D0%B0#cite_note-Bauer-1). Друг Уитстона лорд Лайон Плейфер рекомендовал этот шифр для использования высшими государственными и военными деятелями. Однако [Министерство иностранных дел Великобритании](https://ru.wikipedia.org/wiki/%D0%9C%D0%98%D0%94_%D0%92%D0%B5%D0%BB%D0%B8%D0%BA%D0%BE%D0%B1%D1%80%D0%B8%D1%82%D0%B0%D0%BD%D0%B8%D0%B8) отклонило этот документ из-за сложности его восприятия.

Шифр использовался в тактических целях [британскими](https://ru.wikipedia.org/wiki/%D0%92%D0%B5%D0%BB%D0%B8%D0%BA%D0%BE%D0%B1%D1%80%D0%B8%D1%82%D0%B0%D0%BD%D0%B8%D1%8F) вооруженными силами во [Второй Англо-Бурской войне](https://ru.wikipedia.org/wiki/%D0%92%D1%82%D0%BE%D1%80%D0%B0%D1%8F_%D0%B0%D0%BD%D0%B3%D0%BB%D0%BE-%D0%B1%D1%83%D1%80%D1%81%D0%BA%D0%B0%D1%8F_%D0%B2%D0%BE%D0%B9%D0%BD%D0%B0) и в [Первой мировой войне](https://ru.wikipedia.org/wiki/%D0%9F%D0%B5%D1%80%D0%B2%D0%B0%D1%8F_%D0%BC%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D1%8F_%D0%B2%D0%BE%D0%B9%D0%BD%D0%B0), а также [австралийцами](https://ru.wikipedia.org/wiki/%D0%90%D0%B2%D1%81%D1%82%D1%80%D0%B0%D0%BB%D0%B8%D1%8F) и [немцами](https://ru.wikipedia.org/wiki/%D0%93%D0%B5%D1%80%D0%BC%D0%B0%D0%BD%D0%B8%D1%8F) во время [Второй мировой войны](https://ru.wikipedia.org/wiki/%D0%92%D1%82%D0%BE%D1%80%D0%B0%D1%8F_%D0%BC%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D1%8F_%D0%B2%D0%BE%D0%B9%D0%BD%D0%B0). Причиной использования шифра Плейфера была его достаточная простота в применении и отсутствие необходимости в дополнительном специальном оборудовании. Основной целью использования этой системы шифрования была защита важной, но несекретной информации во время ведения боя. К тому времени, когда вражеские криптоаналитики взламывали сообщение, информация уже была бесполезна для них[[1]](https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80_%D0%9F%D0%BB%D0%B5%D0%B9%D1%84%D0%B5%D1%80%D0%B0#cite_note-Bauer-1)[[3]](https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80_%D0%9F%D0%BB%D0%B5%D0%B9%D1%84%D0%B5%D1%80%D0%B0#cite_note-:0-3).

Использование шифра Плейфера в настоящее время является нецелесообразным, поскольку современные [компьютеры](https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80) могут легко взломать шифр в течение нескольких секунд

Шифр Плейфера использует матрицу 5х5 (для латинского алфавита, для кириллического алфавита необходимо увеличить размер матрицы до 4х8), содержащую ключевое слово или фразу. Для создания матрицы и использования шифра достаточно запомнить ключевое слово и четыре простых правила. Чтобы составить ключевую матрицу, в первую очередь нужно заполнить пустые ячейки матрицы буквами ключевого слова (не записывая повторяющиеся символы), потом заполнить оставшиеся ячейки матрицы символами алфавита, не встречающимися в ключевом слове, по порядку (в английских текстах обычно опускается символ «Q», чтобы уменьшить алфавит, в других версиях «I» и «J» объединяются в одну ячейку). Ключевое слово может быть записано в верхней строке матрицы слева направо, либо по спирали из левого верхнего угла к центру. Ключевое слово, дополненное алфавитом, составляет матрицу 5х5 и является ключом шифра[[5]](https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80_%D0%9F%D0%BB%D0%B5%D0%B9%D1%84%D0%B5%D1%80%D0%B0#cite_note-Stallings-5)[[6]](https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80_%D0%9F%D0%BB%D0%B5%D0%B9%D1%84%D0%B5%D1%80%D0%B0#cite_note-6).

Для того чтобы зашифровать сообщение, необходимо разбить его на биграммы (группы из двух символов), например «Hello World» становится «HE LL OW OR LD», и отыскать эти биграммы в таблице. Два символа биграммы соответствуют углам прямоугольника в ключевой матрице. Определяем положения углов этого прямоугольника относительно друг друга. Затем, руководствуясь следующими 4 правилами[[5]](https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80_%D0%9F%D0%BB%D0%B5%D0%B9%D1%84%D0%B5%D1%80%D0%B0#cite_note-Stallings-5), зашифровываем пары символов исходного текста:

1. Если два символа биграммы совпадают (или если остался один символ), добавляем после первого символа «Х», зашифровываем новую пару символов и продолжаем. В некоторых вариантах шифра Плейфера вместо «Х» используется «Q».

2. Если символы биграммы исходного текста встречаются в одной строке, то эти символы замещаются на символы, расположенные в ближайших столбцах справа от соответствующих символов. Если символ является последним в строке, то он заменяется на первый символ этой же строки.

3. Если символы биграммы исходного текста встречаются в одном столбце, то они преобразуются в символы того же столбца, находящиеся непосредственно под ними. Если символ является нижним в столбце, то он заменяется на первый символ этого же столбца.

4. Если символы биграммы исходного текста находятся в разных столбцах и разных строках, то они заменяются на символы, находящиеся в тех же строках, но соответствующие другим углам прямоугольника.

Для расшифровки необходимо использовать инверсию этих четырёх правил, откидывая символы «Х» (или «Q»), если они не несут смысла в исходном сообщении.

Как и большинство шифров формальной криптографии, шифр Плейфера также может быть легко взломан, если имеется достаточный объём текста. Получение ключа является относительно простым, если известны шифрованный и обычный текст. Когда известен только зашифрованный текст, криптоаналитики анализируют соответствие между частотой появления биграмм в зашифрованном тексте и известной частотой появления биграмм в языке, на котором написано сообщение.

**Шифр Уитсона** или **Шифр двойного квадрата** — ручная [симметрическая](https://ru.wikipedia.org/wiki/%D0%A1%D0%B8%D0%BC%D0%BC%D0%B5%D1%82%D1%80%D0%B8%D1%87%D0%BD%D1%8B%D0%B5_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D1%8B) техника шифрования, изобретенная английским физиком [Чарльзом Уитстоном](https://ru.wikipedia.org/wiki/%D0%A3%D0%B8%D1%82%D1%81%D1%82%D0%BE%D0%BD,_%D0%A7%D0%B0%D1%80%D0%BB%D1%8C%D0%B7) в 1854 году[[1]](https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80_%D0%A3%D0%B8%D1%82%D1%81%D1%82%D0%BE%D0%BD%D0%B0#cite_note-I20-1). Свое название шифр получил из-за схожести с [квадратом Полибия](https://ru.wikipedia.org/wiki/%D0%9A%D0%B2%D0%B0%D0%B4%D1%80%D0%B0%D1%82_%D0%9F%D0%BE%D0%BB%D0%B8%D0%B1%D0%B8%D1%8F). Данная система шифрования является улучшенной версией [шифра Плейфера](https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80_%D0%9F%D0%BB%D0%B5%D0%B9%D1%84%D0%B5%D1%80%D0%B0), в котором аналогичным образом используется замена биграмм (пара символов), но только с помощью одного квадрата.

Для шифрования методом Уитстона используется две матрицы 5x5 (для латинского алфавита, для другого алфавита могут использоваться другого размера матрицы, не обязательно квадратные), которые находятся либо одна под другой в (вертикальном варианте), либо друг напротив друга (в горизонтальном). Каждая из матриц в первую очередь заполняется соответствующим ключевым словом, не записывая повторяющиеся буквы, затем в оставшиеся ячейки матрицы записываются по порядку символы алфавита, которые не были ранее использованы (обычно буква «Q» опускаются, чтобы уменьшить алфавит, либо «I» и «J» объединяются в одной клетке). Ключевое слово может быть записано двумя способами: либо в верхней строке матрицы слева направо, либо по спирали из левого верхнего угла к центру. Таким образом полностью заполняется матрица 5х5. Стоит отметь, что ключ шифра Уитстона, как правило, состоит из двух слов (по одному слову на каждую матрицу), но может состоять и из одного слова и использовано только для первой матрицы

<https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80_%D0%9F%D0%BB%D0%B5%D0%B9%D1%84%D0%B5%D1%80%D0%B0>

<https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80_%D0%A3%D0%B8%D1%82%D1%81%D1%82%D0%BE%D0%BD%D0%B0>