Криптография это интересная наука о шифрахДве алфавитные последовательности, используемые в процессе шифрования, называются, соответственно, открытым и шифровальным компонентом системы. Чтобы получатель шифрограммы мог восстановить открытый текст и прочитать сообщение, ему необходимо иметь копию вышеприведенной таблицы. Дешифровщик повторяет в обратном порядке все действия шифровальщика, раскрывая тем самым содержание сообщения.

В вышеприведенном примере использовался алгоритм побуквенной замены. Этот метод называется простой, или моноалфавитной заменой. Ключ к данному шифру состоит из таблицы, содержащей открытый и шифровальный алфавиты, в которой указывается, на какую букву в шифротексте следует заменить букву открытого текста. В такой криптографической системе предполагается, что алгоритм шифрования общеизвестен, тогда как ключ доступен только отправителю и получателю соответствующих сообщений.

В открытом алфавите буквы расположены в их обычной последовательности; такой алфавит называется прямой стандартной последовательностью. Шифровальный же алфавит в нашем примере состоит из 26 букв латинского алфавита, определенным образом переставленных с использованием ключевого слова BLUESTOCKING (букв. «синий чулок»). После ключевого слова (ключевой фразы) ключ далее записывается с опущением всех тех букв, что уже появились в этом слове (или в первом слове этой фразы), а затем вписываются остающиеся буквы алфавита в обычном порядке, опять же с опущением всех ранее появившихся букв. Так, если в качестве ключевой мы используем фразу UNITED STATES OF AMERICA, то шифровальный алфавит будет выглядеть следующим образом:

U N I T E D S A O F M R C B G H J K L P Q V W X Y Z

С помощью ключевого слова (фразы) при шифровании можно перемешать любую алфавитную последовательность. Использование ключевых слов облегчает восстановление открытого и шифровального компонента системы, поскольку при этом необходимо запомнить только соответствующее ключевое слово (фразу). Нет необходимости записывать (или разгадывать) какие бы то ни было таблицы: если помнить ключевое слово, то алфавитную последовательность всегда можно восстановить по памяти.

В вышеприведенной шифрограмме между словами сохранены пробелы, однако шифровку можно сделать более защищенной (или, как говорят криптографы, устойчивой, или стойкой ко взлому; шифр считается тем более стойким, чем дольше он не поддается вскрытию) путем удаления межсловных пробелов из окончательного шифротекста. Согласно установившейся практике, шифротекст принято делить на группы из пяти букв каждая. (Когда-то телеграфные компании при взимании платы каждую группу из пяти букв считали как одно слово открытого текста.) Если убрать пробелы между словами, то нашу шифрограмму можно было бы записать так: