Для початку роботи шифру Вернама потрібно виписати весь алфавіт, та проставити біля кожного символу унікальний двійковий код(однакової довжини). Після чого, замінити в тексті символи на двійкові коди. Далі потрібно створити ключ. Ключем буде послідовність випадкових двійкових чисел. Їх кількість потрібна дорівнювати кількості символів в тексті.

Вийшло два рядки. В першому написані двійкові числа, якими замінили символи в тексті, а в другому рядку написано стільки ж випадкових двійкових чисел(довжина кожного числа в першому та другому рядках – однакова). Після цього потрібно застосувати операцію до кожної пари -их елементу в першому та другому рядах. Отримані числа й будуть шифротекстом.

У цього шифру є багато недоліків. По перше, для його роботи потрібен ключ, довжина якого дорівнює довжині тексту. По друге, кожен елемент в ключі потрібен бути випадковим(не псевдовипадковим). А, як відомо, будь який алгоритм, що генерує послідовність є псевдовипадковим, тому потрібно щось, дійсно, випадкове. Наприклад, радіоактивний розпад, чи створений електрогенератором білий шум. Також не можна використовувати одні й ті самі випадкові числа кілька разів поспіль. Ще, при великих розмірах тексту потрібно мати велуку кількість випадкових чисел. Наприклад для тексту із ста слів може потребуватись кількасот випадкових чисел.

Для шифру Вернама доведена його абсолютна криптостійкість. Іншими словами, якщо хтось перехопить повідомлення, то єдиний спосіб дізнатися текст – повний перебір ключа. Біля того, цей шифр – єдиний шифр для якого була доведена абсолютна криптостійкість. Але з цього випливає інша проблема. Якщо канал зв’язку прослуховується, то для кожного наступного повідомлення потрібно мати нові випадкові числа обом сторонам, але тоді вони не зможуть їх передати. Натомість, якщо канал зв’язку не прослуховується, то й в шифруванні повідомлень нема ніякого сенсу. Саме тому цей алгоритм припинили використовувати.