**МЕТОДЫ АНАЛИТИЧЕСКИХ ПРЕОБРАЗОВАНИЙ**

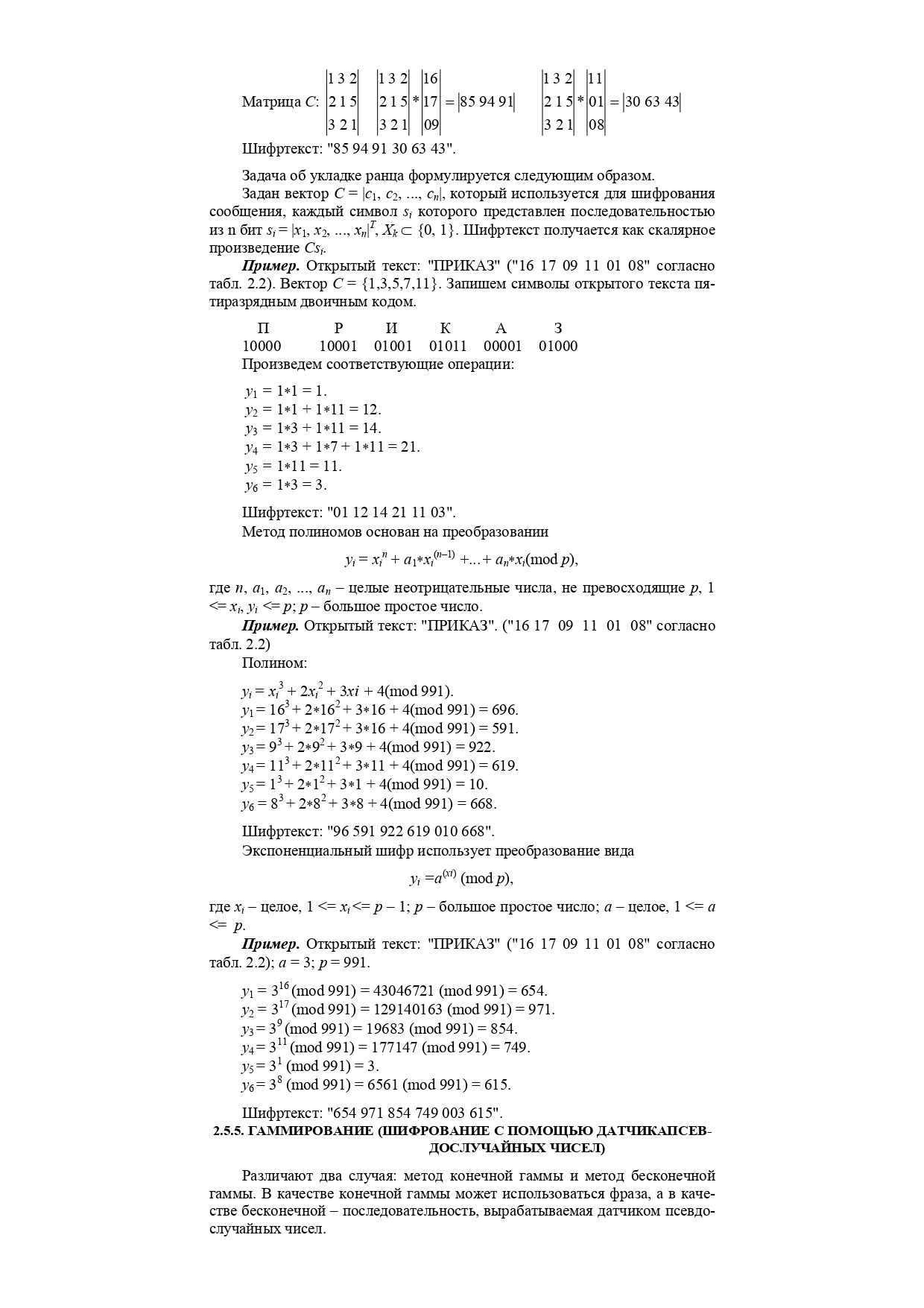
Шифрование методами аналитических преобразований основано на понятии односторонней функции. Будем говорить, что функция *у* = *f* (*х*) является односторонней, если она за сравнительно небольшое число опера- ций преобразует элемент открытого текста *Х* в элемент шифртекста *Y* для всех значений *Х* из области определения, а обратная операция (вычисление *X* = *F*-1(*Y*) при известном шифртексте) является вычислительно трудоемкой. В качестве односторонней функции можно использовать следующие преобразования: умножение матриц; решение задачи об укладке ранца; вычисление значения полинома по модулю; экспоненциальные преобразования и др.

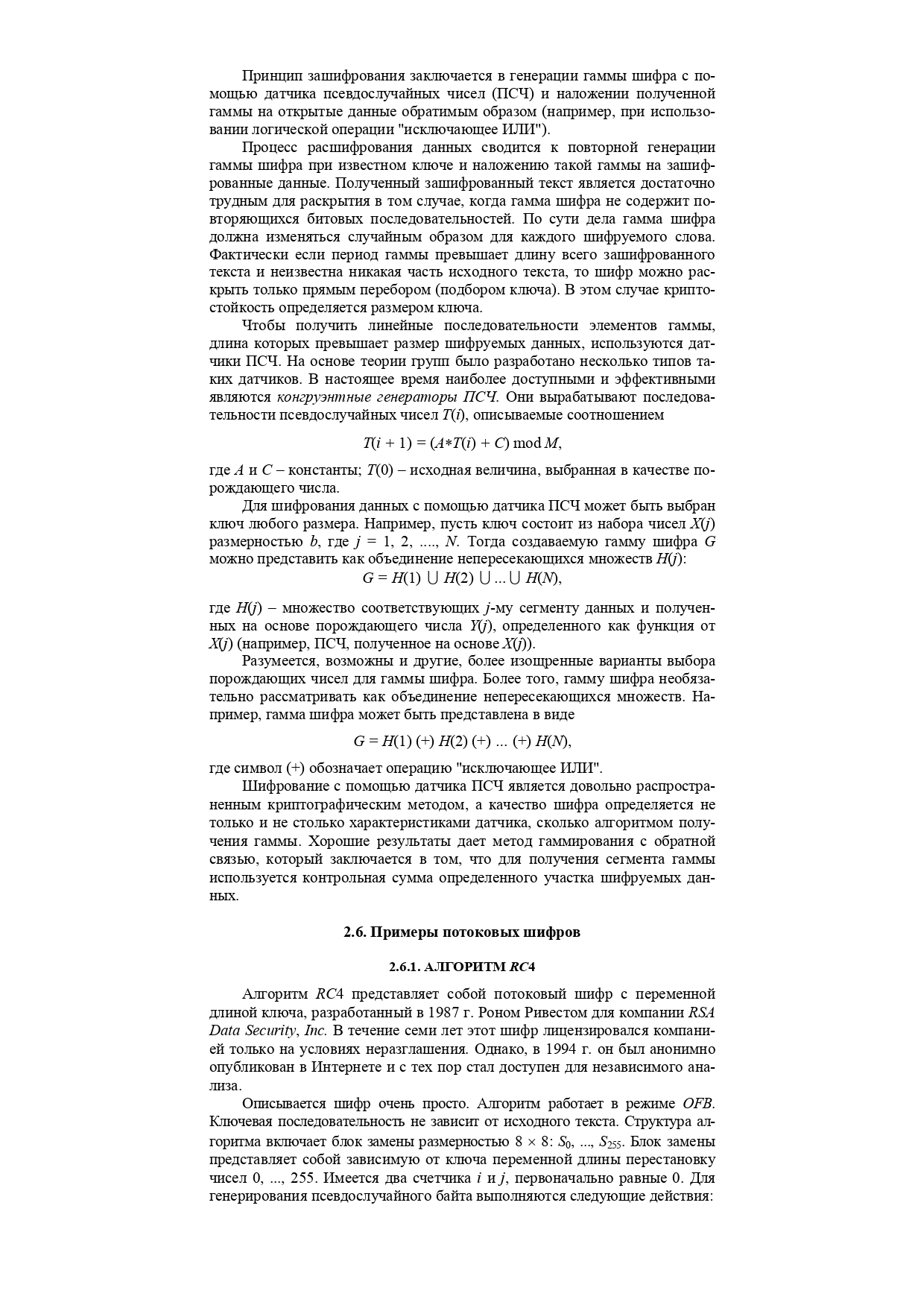
Метод умножения матриц использует преобразование вида

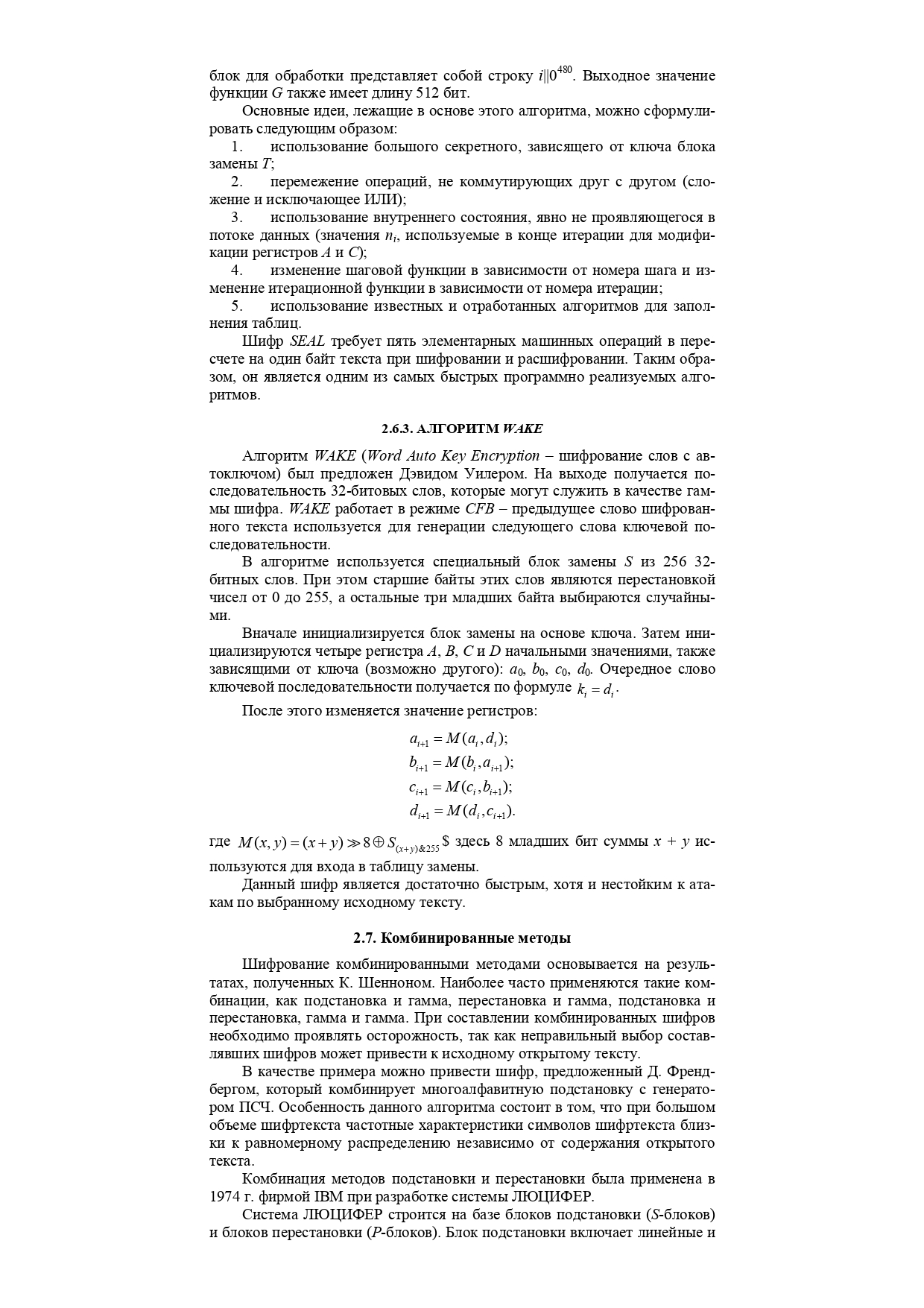
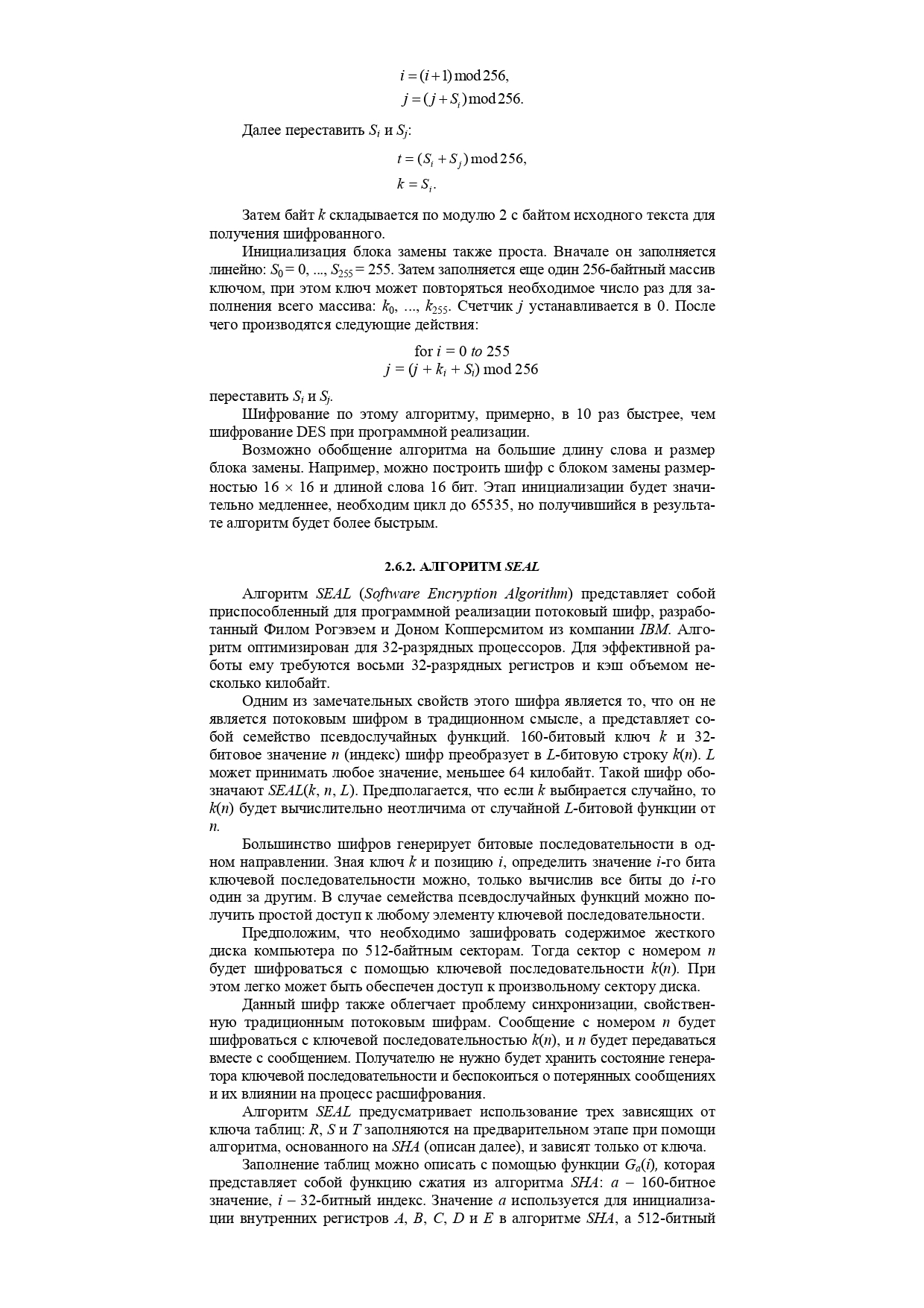
*Y = CX*, где *Y* = ||*y*1, *y*2, ..., *yn*||*Т*; *С* = ||*Cij*||; *X* = ||*x*1, *x*2, ..., *xn*||.

***Пример*.** Открытый текст: "ПРИКАЗ" ("16 17 09 11 01 08" согласно

табл. 2.2).







Задание (варианты).

1. Шифрование методами аналитических преобразований.
2. Шифрование алгоритмом WEKE.
3. Шифрование алгоритмом SEAL.
4. Шифрование алгоритмом RC4.
5. Шифрование алгоритмом.
6. Гаммирование.
7. Шифрование методами аналитических преобразований.
8. Шифрование алгоритмом WEKE.
9. Шифрование алгоритмом SEAL.
10. Шифрование алгоритмом RC4.
11. Шифрование алгоритмом.
12. Гаммирование. Шифрование методами аналитических преобразований.
13. Шифрование алгоритмом WEKE.
14. Шифрование алгоритмом SEAL.
15. Шифрование алгоритмом RC4.
16. Шифрование алгоритмом.
17. Гаммирование.