Защита электронной документации

Методы замены

- Шифрование основано на алгебраическом преобразовании, называемой подстановкой.
- Подстановка – взаимно-однозначное отображение некоторого множества M на себя.
- Моноалфавитная замена. Каждой букве алфавита открытого текста ставится в соответствие одна буква шифротекста из этого же алфавита.
- Общая формула моноалфавитной замены:

$$Y_i = K_1 X_i + K_2 \pmod{n},$$

- где: Y_i - символ алфавита;
- X_i – символ открытого текста;
- n - длина используемого алфавита;
- K_1, K_2 – константы.

Шифр Вижинера

- Шифр Вижинера задается формулой
- $Y_i = X_i + K_i \pmod n$, $X_i = Y_i + K_i \pmod n$,
- где K_i - i , буква ключа (слово или фраза).
- Пример: Открытый текст ЗАМЕНА

8	1	13	6	14	1
З	А	М	Е	Н	А
К	Л	Ю	Ч	К	Л
11	12	31	24	11	12

- Y1 = 8 + 11(mod33) = 19 (Т) X1 = 19 - 11(mod33) = 8 (З)
- Y2 = 1 + 12(mod33) = 13 (М)
- Y3 =13 + 31(mod33) = 11 (К)
- Ответ: зашифрованный текст - ТМКЭШМ

Формирование ПСП

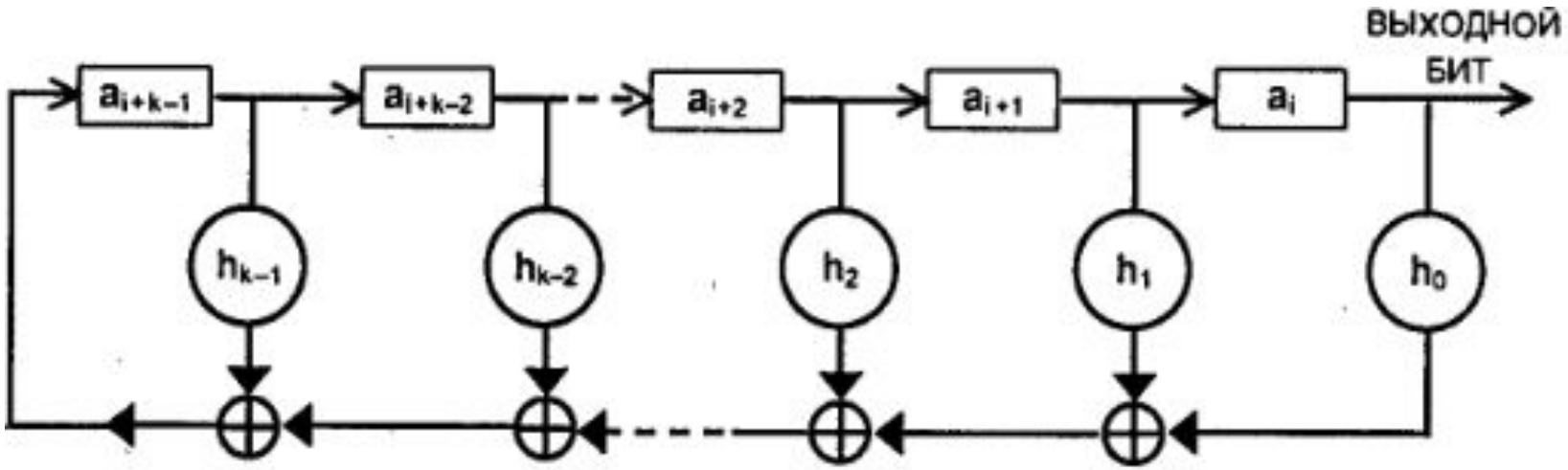
- Методы формирования ПСП чисел
- 1. Джон фон Нейман (1946 г): каждое последующее число образуется возведением в квадрат предыдущего числа с отбрасыванием цифр младших и старших разрядов.
- 2. Линейный конгруэнтный генератор использует соотношение
  - $Y_i = (a\, Y_{i-1} + b) \bmod m,$
- где: a, b – константы;
- m – модуль;
- Y_0 – исходное значение.

Формирование ПСП

- 3. Генерация ПСП на основе рекуррентных соотношений:

$$\sum_{j=0}^{k} hjai = 0$$

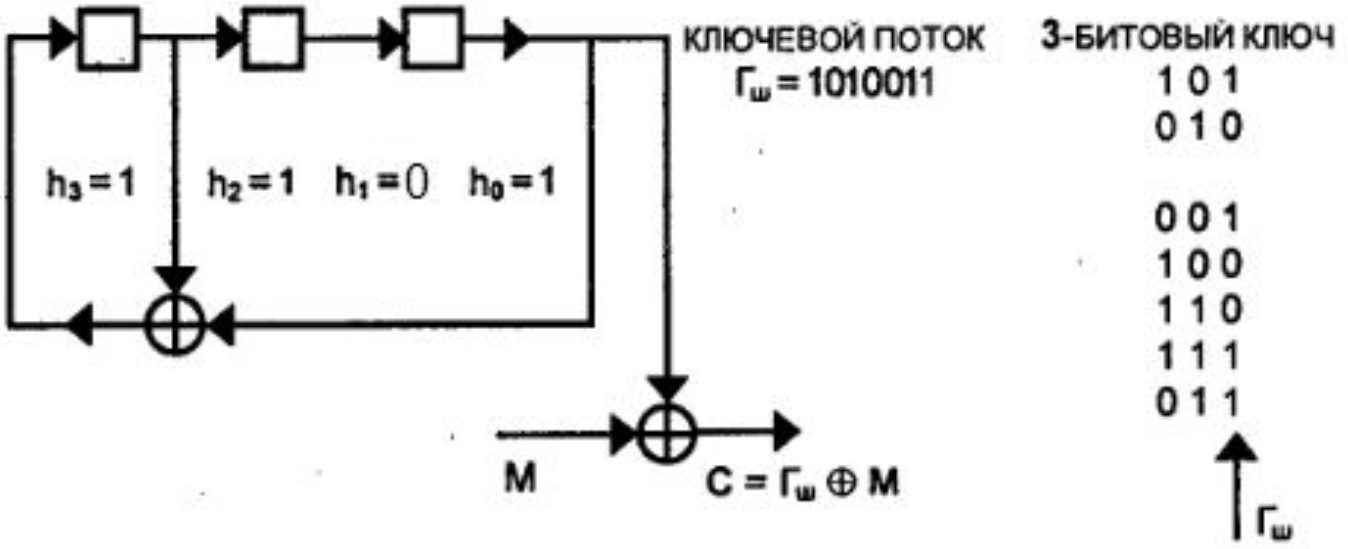
- Схема генератора с регистром сдвига



Формирование ПСП

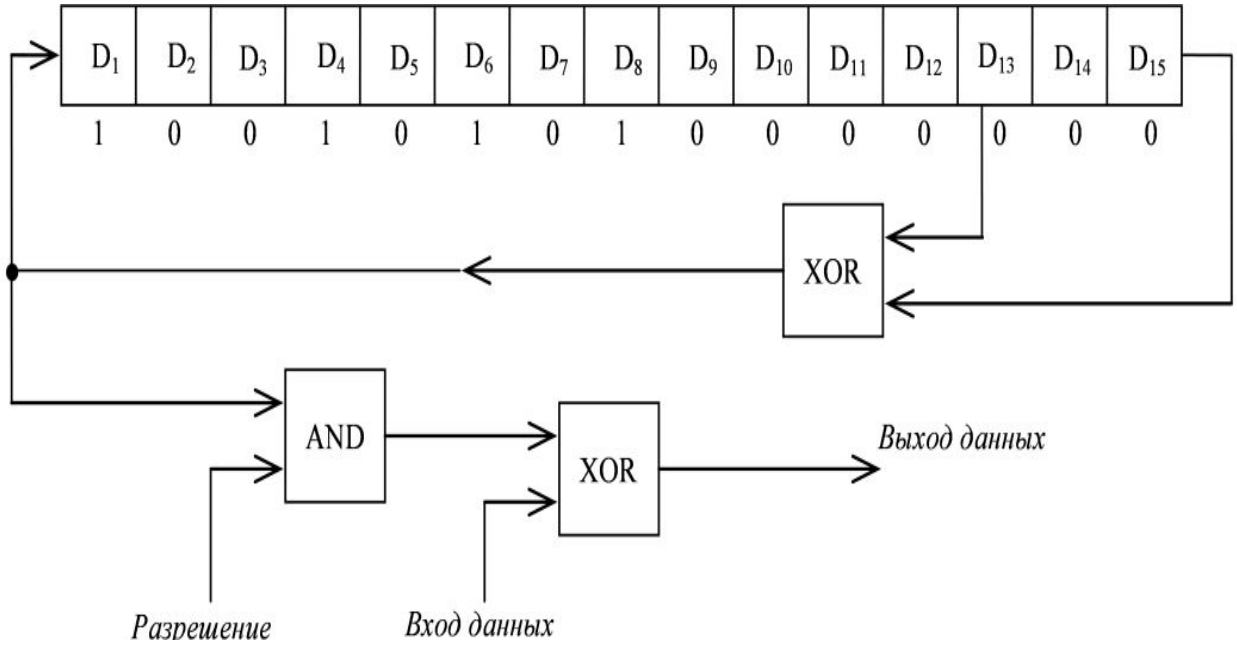
Трехразрядный сдвиговый регистр с линейной обратной связью, построенный в соответствии с полиномом:

- $h(x) = X^3 + X^2 + 1$,
- где коэффициенты $h_3 = 1$, $h_2 = 1$, $h_1 = 0$, $h_0 = 1$.



Формирование ПСП

- Генератор ПСП на регистрах сдвига.

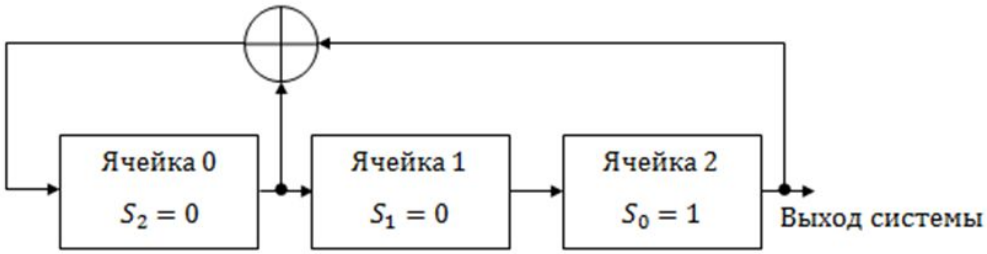


- В генераторе ПСП скремблера используется полином:
-
- $$G(D) = 1 + X^{13} + X^{15}.$$

Пример последовательности

- Конфигурация Фибоначчи
- Регистр сдвига с линейной обратной связью задаётся $X^3 + X + 1$ характеристическим многочленом. Состояния регистра приведены в таблице.

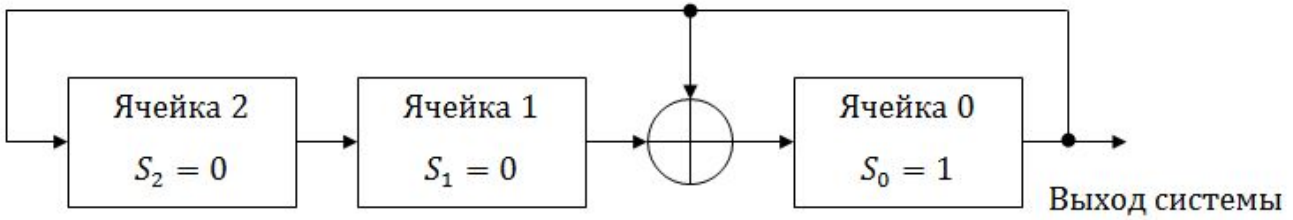
Номер шага	Состояние	Генерируемый бит
0	[0, 0, 1]	-
1	[1, 0, 0]	1
2	[1, 1, 0]	0
3	[1, 1, 1]	0
4	[0, 1, 1]	1
5	[1, 0, 1]	1
6	[0, 1, 0]	1
7	[0, 0, 1]	0



- https://ru.wikipedia.org/wiki/Регистр_сдвига_с_линейной_обратной_связью

Конфигурация Галуа

- Возьмем многочлен, у которого: C3 = C1 = 1, C2 = 0.



- Длина последовательности
- 7 бит.

Номер шага	Состояние	Генерируемый бит
0	[0, 0, 1]	-
1	[1, 0, 1]	1
2	[1, 1, 1]	1
3	[1, 1, 0]	1
4	[0, 1, 1]	0
5	[1, 0, 0]	1
6	[0, 1, 0]	0
7	[0, 0, 1]	0

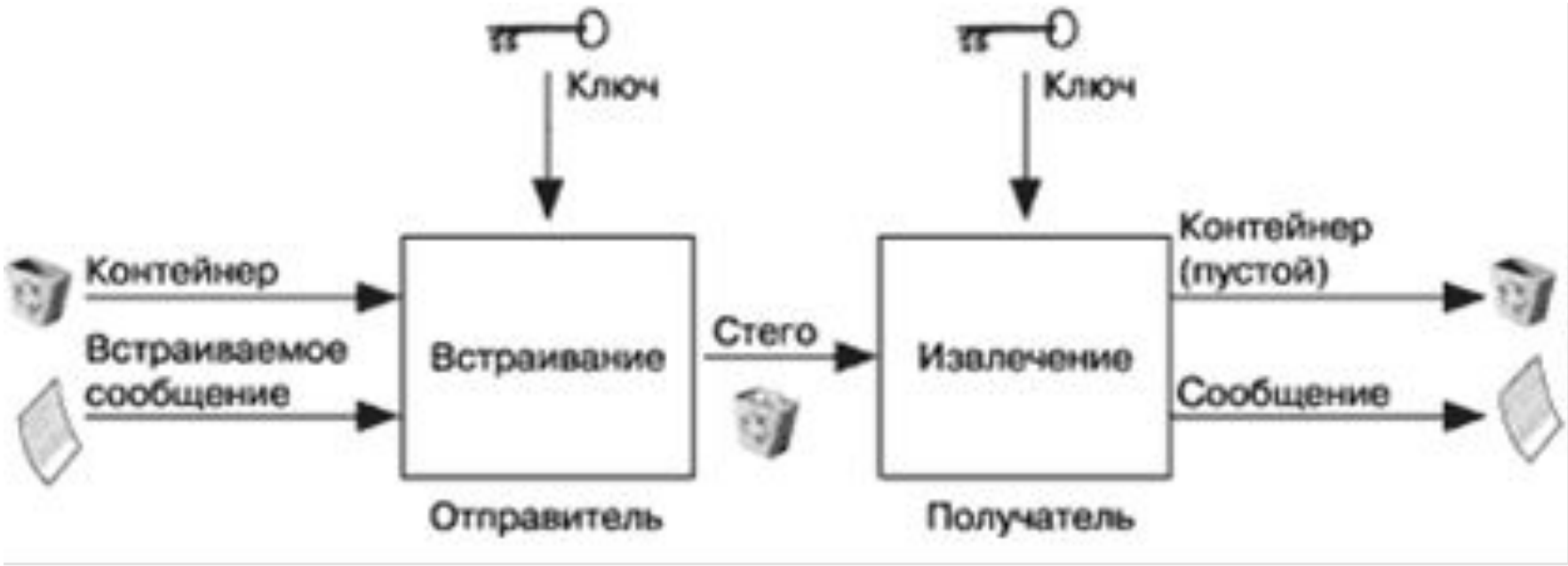
Генерация примитивных многочленов

https://ru.wikipedia.org/wiki/Регистр_сдвига_с_линейной_обратной_связью

Биты, n	Примитивный многочлен	Период, $2^n - 1$	Число примитивных многочленов
2	$x^2 + x + 1$	3	1
3	$x^3 + x^2 + 1$	7	2
4	$x^4 + x^3 + 1$	15	2
5	$x^5 + x^3 + 1$	31	6
6	$x^6 + x^5 + 1$	63	6
7	$x^7 + x^6 + 1$	127	18
8	$x^8 + x^6 + x^5 + x^4 + 1$	255	16
9	$x^9 + x^5 + 1$	511	48
10	$x^{10} + x^7 + 1$	1023	60
11	$x^{11} + x^9 + 1$	2047	176
12	$x^{12} + x^{11} + x^{10} + x^4 + 1$	4095	144
13	$x^{13} + x^{12} + x^{11} + x^8 + 1$	8191	630
14	$x^{14} + x^{13} + x^{12} + x^2 + 1$	16383	756
15	$x^{15} + x^{14} + 1$	32767	1800
16	$x^{16} + x^{14} + x^{13} + x^{11} + 1$	65535	2048
17	$x^{17} + x^{14} + 1$	131071	7710
18	$x^{18} + x^{11} + 1$	262143	7776
19	$x^{19} + x^{18} + x^{17} + x^{14} + 1$	524287	27594

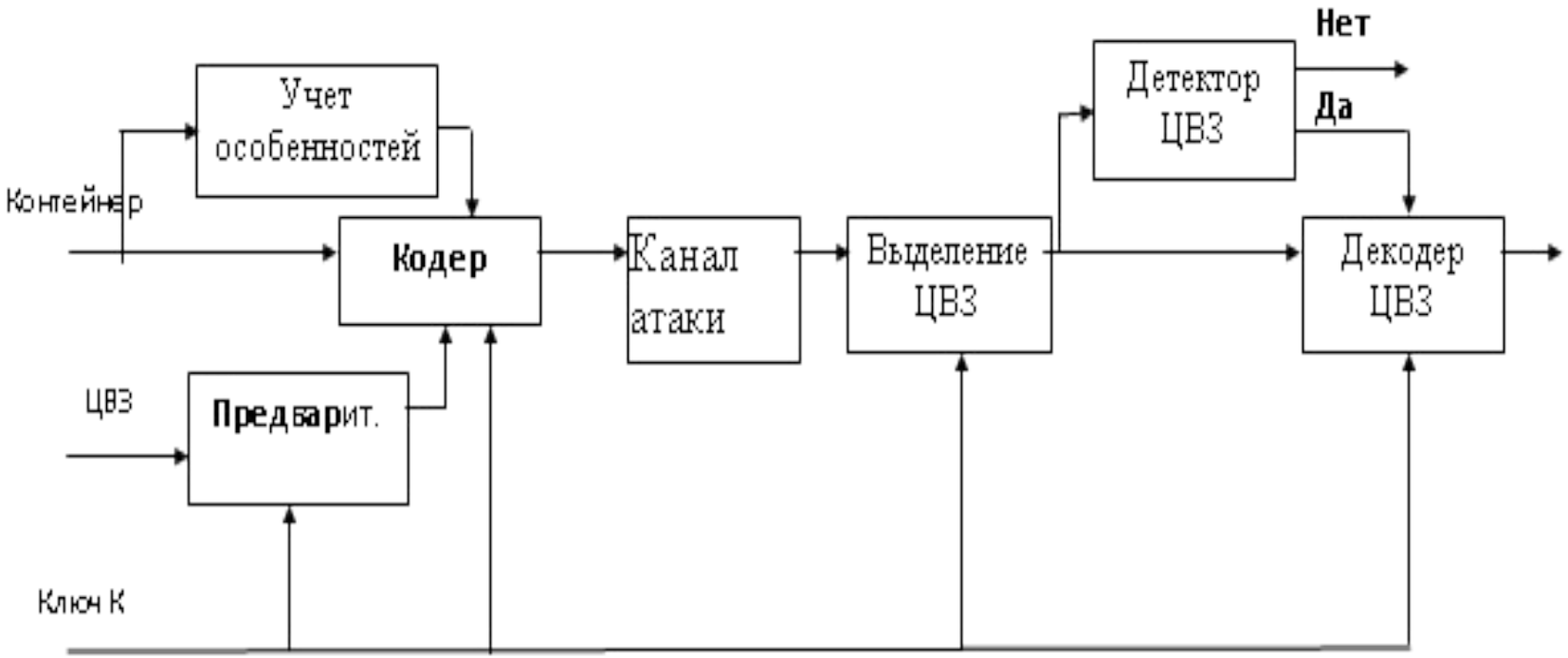
Стеганография

- Стеганографическая система - совокупность средств и методов, которые используются для формирования скрытого канала передачи информации.
- Обобщенная модель стегосистемы.



Цифровые водяные знаки

- Структурная схема системы ЦВЗ



Контрольные вопросы

- 1. Какие существуют методы защиты электронных документов?
- 2. Как осуществляется моноалфавитная замена?
- 3. Как осуществить шифрование заданного текста, используя метод Вижинера?
- 4. Как выполняется шифрование с помощью датчика ПСП?
- 5. Как формируется ПСП?
- 6. Перечислите свойства ПСП
- 7. Что такое генераторный полином?
- 8. Как построить генератор ПСП зная полином?
- 9.Что понимается под цифровой стеганографией?
- 10. Где применяются и как формируются цифровые водяные знаки?

Список использованных источников и литературы

- 1. Петраков А.В. Основы практической защиты информации. — М.: Радио и связь, 1999. - 368 с.
- 2. Казанцев Г.Д. Телевидение и телевизионные устройства: Учебное пособие. − Томск: кафедра ТУ, ТУСУР, 2012. – 216 с.
- 3. Конахович Г. Ф., Пузыренко А.Ю. Компьютерная стеганография. Теория и практика. - К.: «МК-Пресс», 2006. – 280 с.
- 4.https://ru.wikipedia.org/wiki/Регистр_сдвига_с_линейной_обратной_связью