Московский институт электроники и математики им. А.Н. Тихонова

Кафедра информационной безопасности киберфизических систем

Москва 2024

Криптографические методы защиты информации

ГОСТ Р 34.13-2015

Режимы

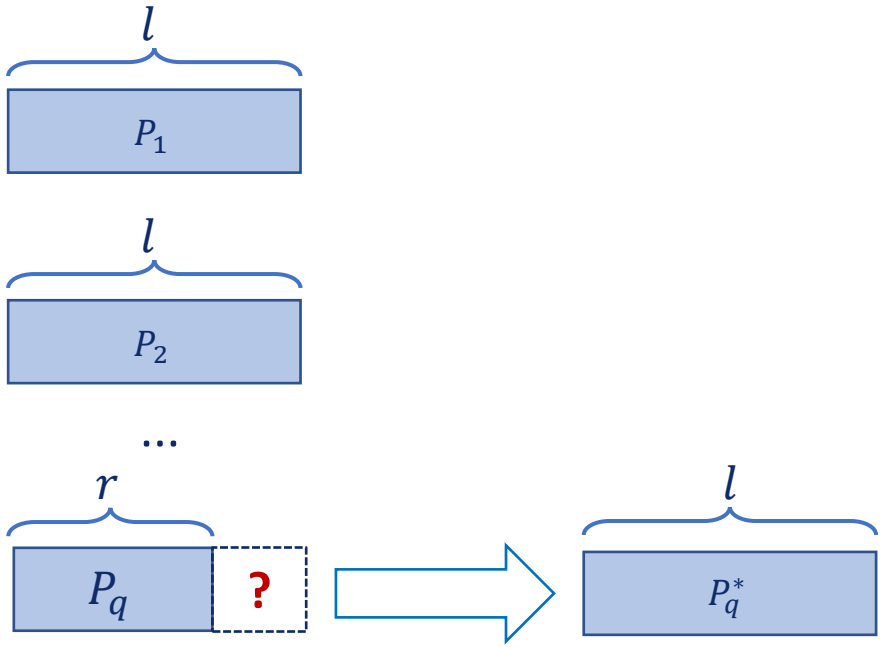
- **Режим простой замены (Electronic Codebook, ECB)**;
- Режим гаммирования (Counter, CTR);
- Режим гаммирования с обратной связью по выходу (Output Feedback, OFB);
- Режим простой замены с зацеплением (Cipher Block Chaining, CBC);
- Режим гаммирования с обратной связью по шифртексту (Cipher Feedback, CFB);
- Режим выработки имитовставки (Message Authentication Code algorithm).

Основные обозначения

0^r	двоичная строка, состоящая из r нулей;
MSB_s	замена двоичной строки ее старшими битами в количестве s;
LSB_s	замена двоичной строки ее младшими битами в количестве s;
n	длина блока базового блочного шифра;
s	длина блока гаммы;
P	открытый текст, $P = P_1 \| \| P_2 \| \| P_3 \| \| \dots \| \| P_q$;
C	шифртекст, $C = C_1 \| \| C_2 \| \| C_3 \| \| \dots \| \| C_q$.

Дополнение сообщения

- Сообщение $P \in V^*$, $|P| \bmod l = r$.



- **Процедура 1:**
  - $P^* = \begin{cases} P, & \text{если } r = 0, \\ P \,||\, 0^{l-r}, & \text{иначе.} \end{cases}$
- **Процедура 2:**
  - $P^* = P \,||\, 1 \,||\, 0^{l-r-1}$
- **Процедура 3:**
  - $P^* = \begin{cases} P, & \text{если } r = n, \\ P \,||\, 1 \,||\, 0^{l-r-1}, & \text{иначе.} \end{cases}$

Выработка начального значения

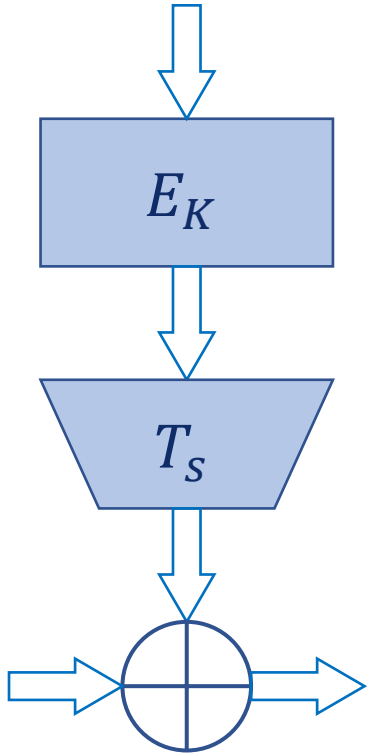
- **Синхропосылка** (**initializing value**) – комбинация знаков, передаваемая по каналу связи и предназначенная для инициализации алгоритма шифрования, а именно: для выработки начального значения вспомогательных переменных, используемых в некоторых режимах работы.

- Требования к синхропосылке:

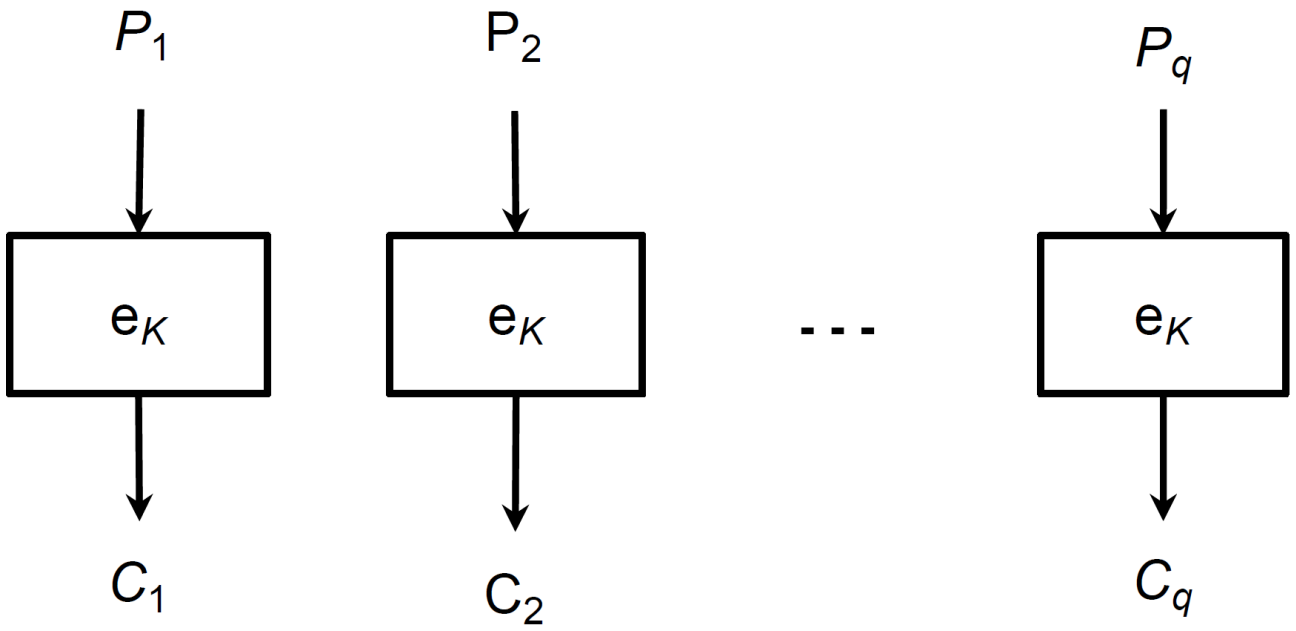
Режим простой замены с зацеплением	Случайность, равновероятность и независимость от других возможных значений.
Режим гаммирования с обратной связью по шифртексту	
Режим гаммирования	Уникальность для сообщений, зашифровываемых на одном ключе.
Режим гаммирования с обратной связью по выходу	Непредсказуемость либо уникальность.

Процедура усечения

- В режимах гаммирования базовый блочный шифр с длиной блока n используется для выработки гаммы, которая блоками длиной $s \leq n$ накладывается на открытый текст:
  - $C_i = P_i \oplus T_s\left(E_K(X_i)\right)$.
- Операция усечения состоит во взятии старших бит блока, выработанного базовым блочным шифром:
  - $T_s = MSB_s$.

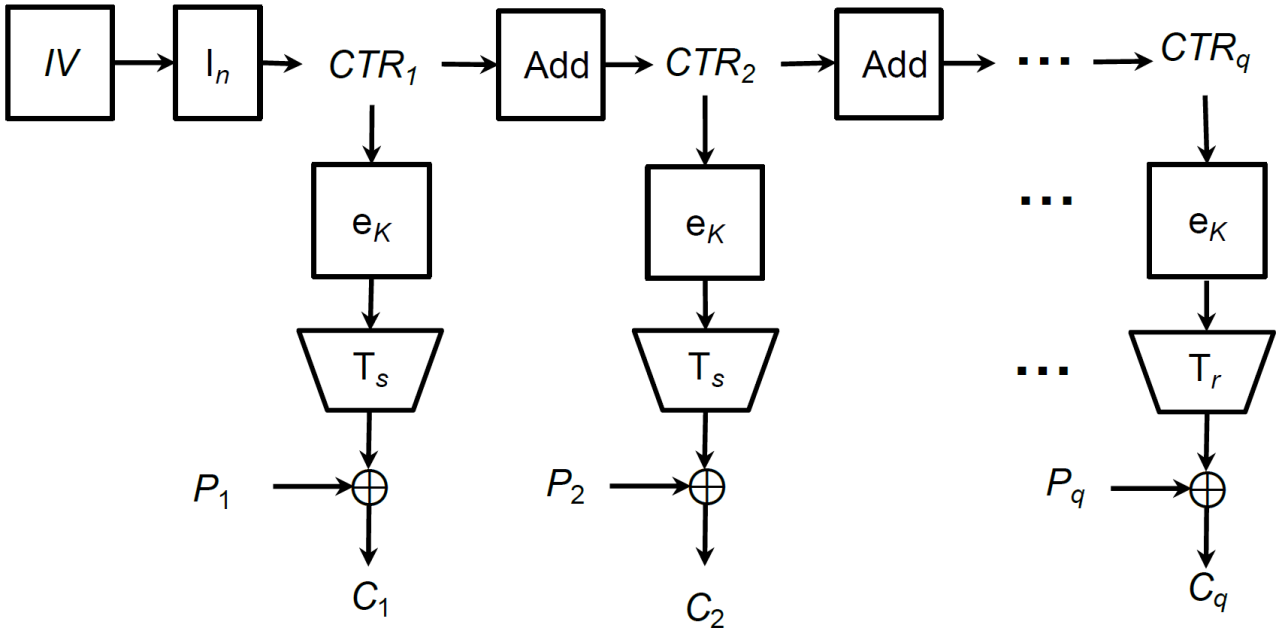


Режим простой замены



- Зашифрование:
  $C_i = \mathrm{E}_K(P_i), \forall i = \overline{1, q}.$

Режим гаммирования



- Зашифрование:

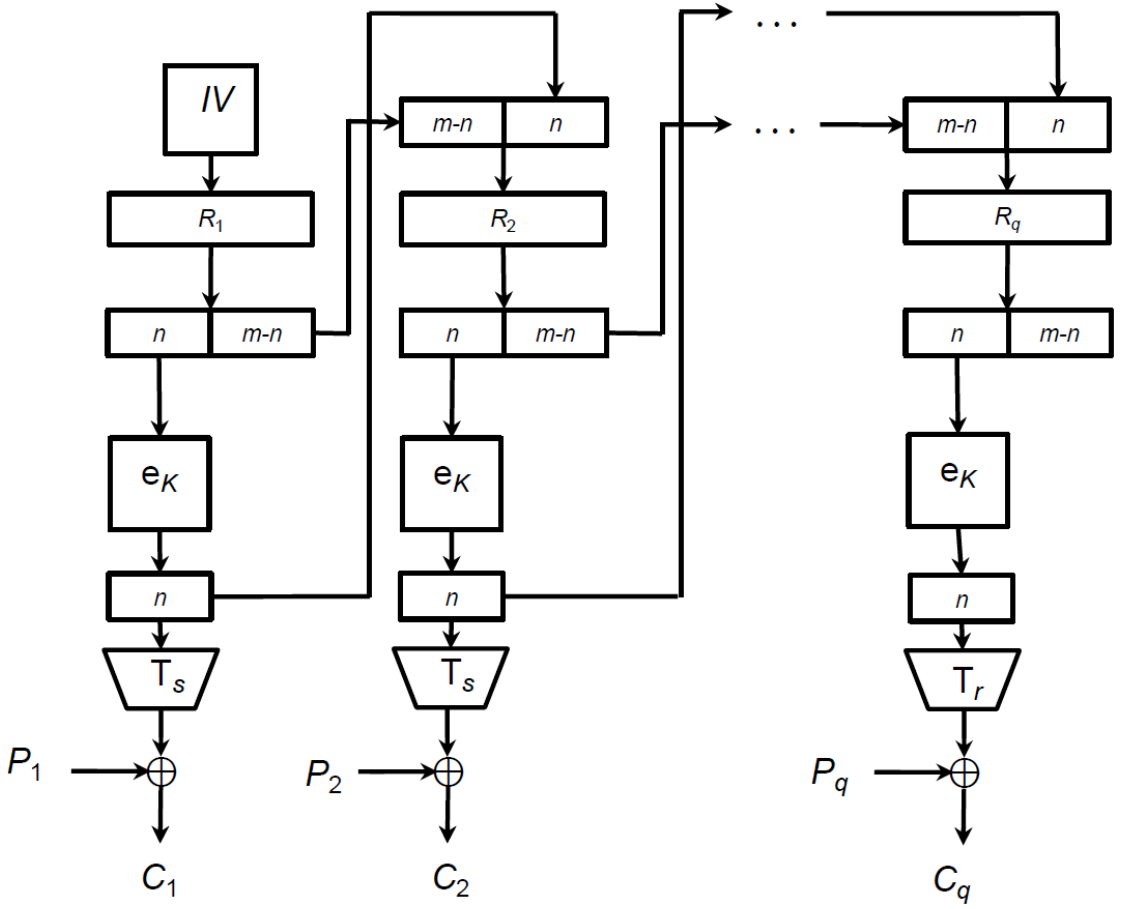
$$CTR_1 = \mathrm{I}_n(IV) = IV \parallel 0^{\frac{n}{2}}, IV \in V_{\frac{n}{2}};$$

$$\forall i = \overline{1, q-1}:$$

$$\begin{cases} CTR_{i+1} = \mathrm{Add}(CTR_i); \\ \mathrm{Add}(CTR_i) = \mathrm{Vec}_n(\mathrm{Int}_n(CTR_i) \boxplus_n 1); \\ C_i = P_i \oplus \mathrm{T}_s\left(\mathrm{E}_K(CTR_i)\right); \end{cases}$$

$$C_q = P_q \oplus \mathrm{T}_r\left(\mathrm{E}_K\left(CTR_q\right)\right).$$

Режим гаммирования с обратной связью по выходу



- Зашифрование:

$$R_1 = IV,\ IV \in V_m,\ m = nz;$$

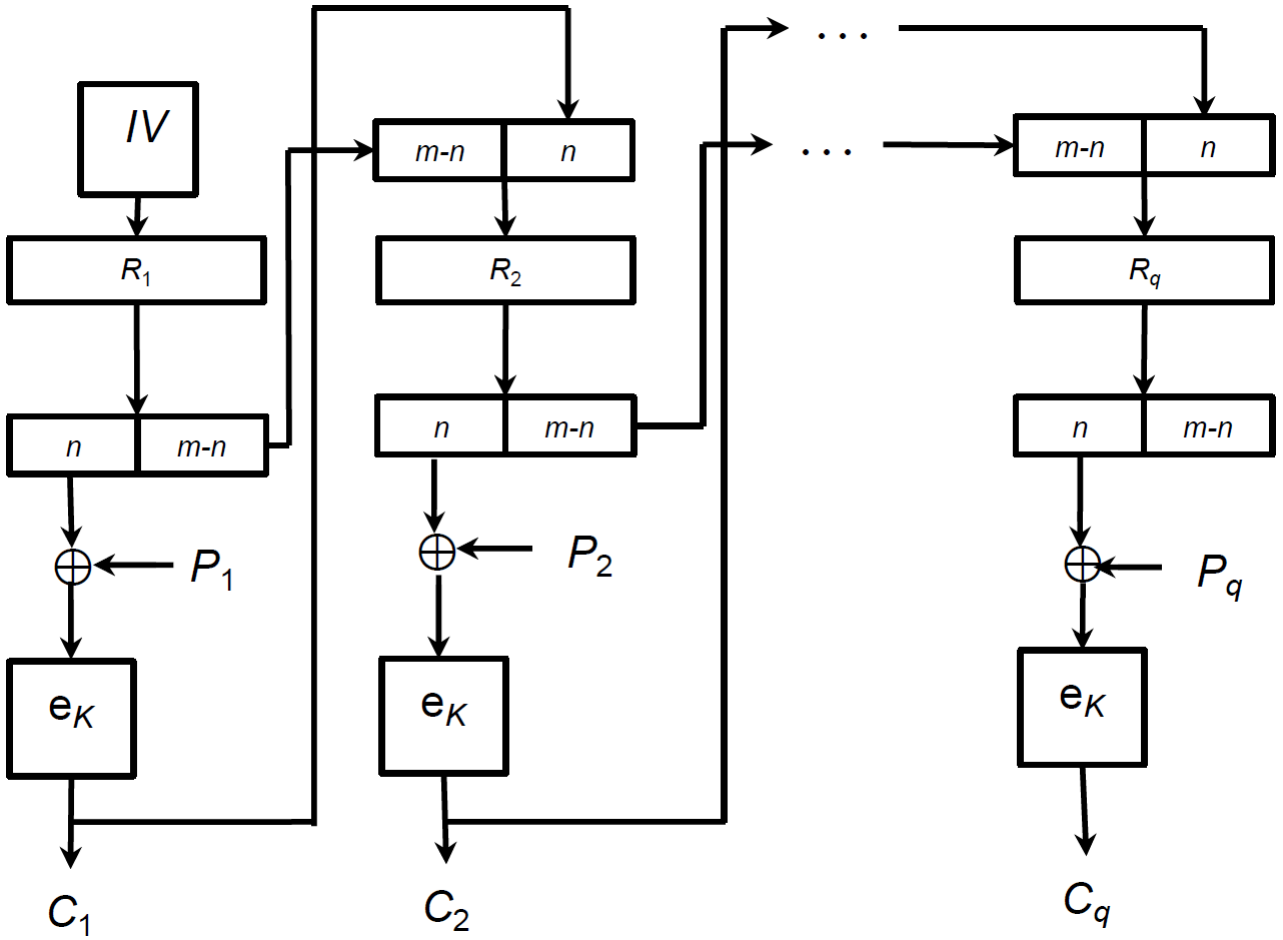
$$\forall i = \overline{1, q-1}:$$

$$\begin{cases} Y_i = \mathrm{E}_K\left(\mathrm{MSB}_n(R_i)\right); \\ C_i = P_i \oplus \mathrm{T}_s(Y_i); \\ R_{i+1} = \mathrm{LSB}_{m-n}(R_i) \parallel Y_i; \end{cases}$$

$$Y_q = \mathrm{E}_K\left(\mathrm{MSB}_n\left(R_q\right)\right);$$

$$C_q = P_q \oplus \mathrm{T}_r\left(Y_q\right).$$

Режим простой замены с зацеплением



- Зашифрование:

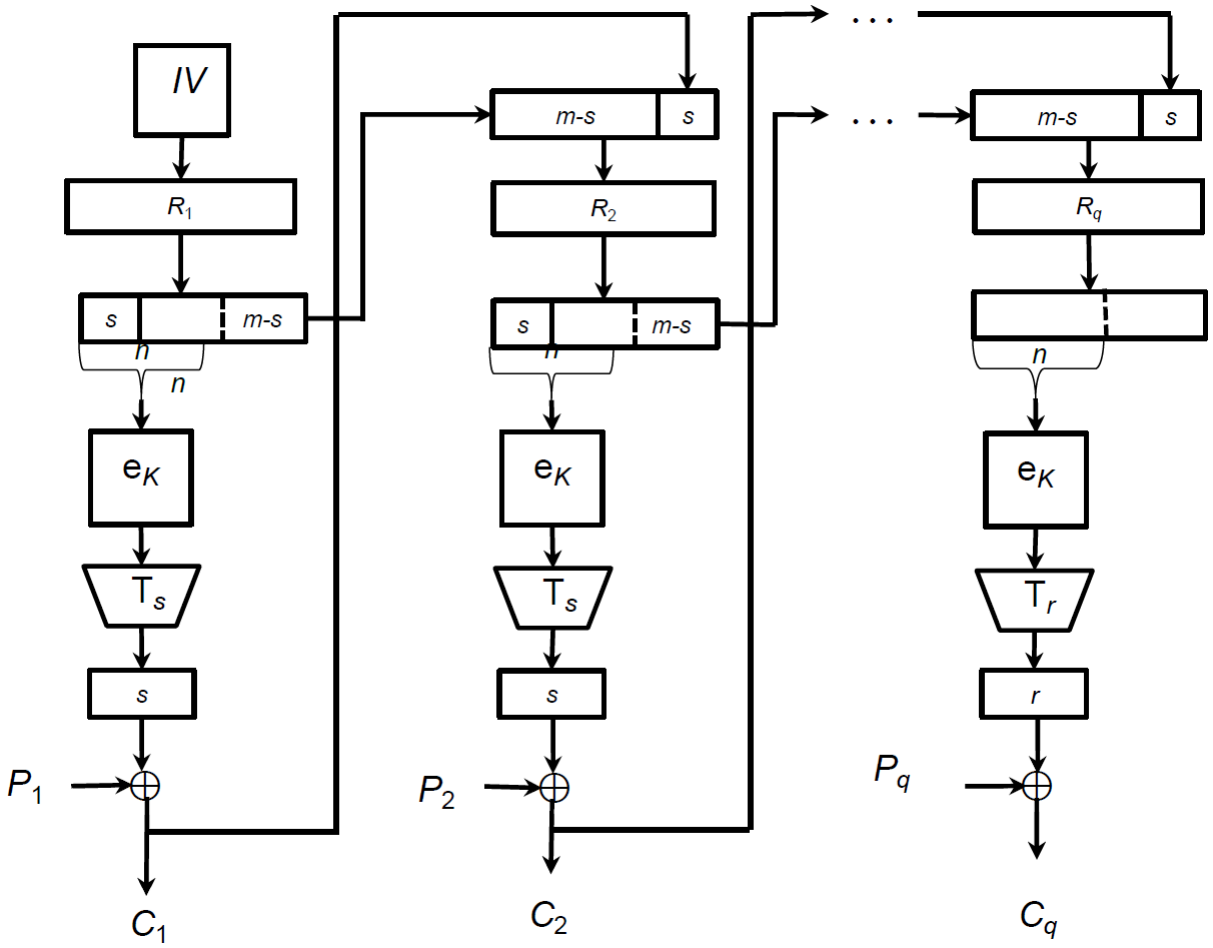
$$R_1 = IV,\ IV \in V_m,\ m = nz;$$

$$\forall i = \overline{1, q-1}:$$

$$\begin{cases} C_i = \mathrm{E}_K\left(P_i \oplus \mathrm{MSB}_n(R_i)\right); \\ R_{i+1} = \mathrm{LSB}_{m-n}(R_i) \parallel C_i; \end{cases}$$

$$C_q = \mathrm{E}_K\left(P_q \oplus \mathrm{MSB}_n(R_q)\right).$$

Режим гаммирования с обратной связью по шифртексту



- Зашифрование:

$R_1 = IV, IV \in V_m, m = nz;$

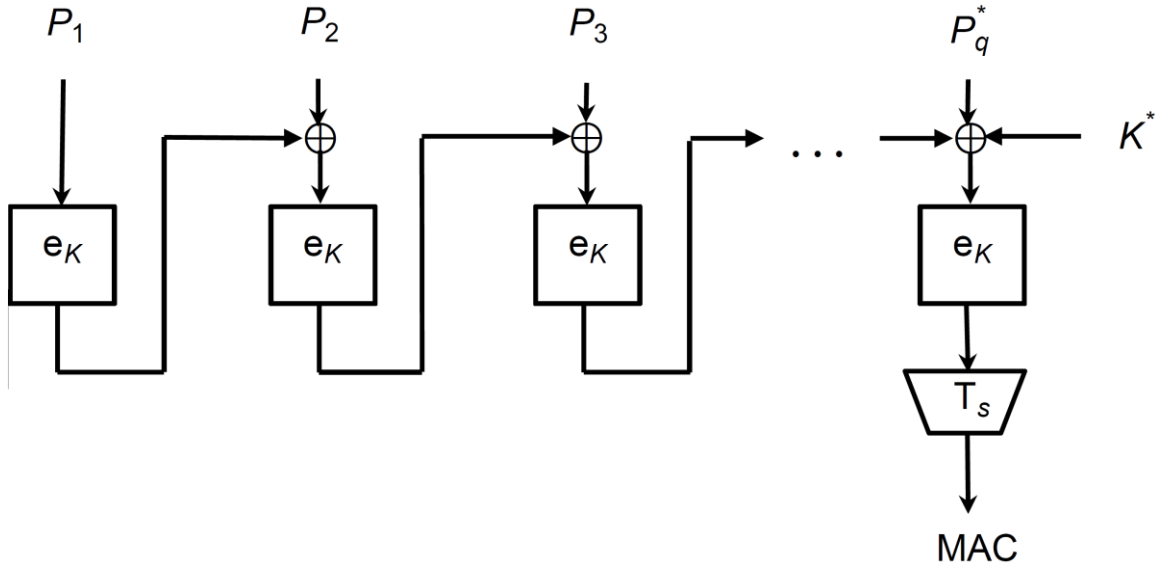
$\forall i = \overline{1, q-1}:$

$$\begin{cases} C_i = P_i \oplus \mathrm{T}_s\left(\mathrm{E}_K\left(\mathrm{MSB}_n(R_i)\right)\right); \\ R_{i+1} = \mathrm{LSB}_{m-s}(R_i) \parallel C_i; \end{cases}$$

$$C_q = P_q \oplus \mathrm{T}_r\left(\mathrm{E}_K\left(\mathrm{MSB}_n(R_q)\right)\right).$$

Режим выработки имитовставки

- **Имитовставка** – это контрольная комбинация, зависящая от открытого текста и секретного ключа, использующаяся для обнаружения всех случайных или преднамеренных изменений в открытом тексте.



$$R = \mathrm{E}_K(0^n);$$

$$K_1 = \begin{cases} R \ll 1, & \text{если } \mathrm{MSB}_1(R) = 0; \\ (R \ll 1) \oplus B_n, & \text{иначе;} \end{cases}$$

$$K_2 = \begin{cases} K_1 \ll 1, & \text{если } \mathrm{MSB}_1(K_1) = 0; \\ (K_1 \ll 1) \oplus B_n, & \text{иначе;} \end{cases}$$

$$B_{64} = 0^{59} \| 11011, B_{128} = 0^{120} \| 10000111;$$

$$C_0 = 0^n;$$

$$C_i = \mathrm{E}_K(P_i \oplus C_{i-1}), i = \overline{1, q-1};$$

$$MAC = \mathrm{T}_s\left(\mathrm{E}_K\left(P_q^* \oplus C_{q-1} \oplus K^*\right)\right);$$

$$K^* = \begin{cases} K_1, & \text{если } |P_q| = n; \\ K_2, & \text{иначе.} \end{cases}$$

Спасибо за внимание!

Евсютин Олег Олегович
Заведующий кафедрой информационной безопасности киберфизических систем
Канд. техн. наук, доцент

+7 923 403 09 21
oevsyutin@hse.ru