

Дедлайн: 21 июня

вариант-1

Кол-во баллов: 12

Реализуйте атаку на шифр Виженера (см. например [\[Алфёров\]](#), с.143, [тест Фридмана](#)) или же на шифр гаммирования с гаммой, генерируемой линейным конгруэнтным генератором псевдослучайных чисел (аффинным генератором).

вариант-2

Кол-во баллов: 7

Реализуйте СРА-КЕМ на базе криптосистемы Мак–Элиса (*т.е. криптосистему Мак–Элиса со случайными сообщениями и ошибками*). В качестве кодов используйте коды Рида–Маллера или коды Рида–Соломона из прошлых индивидуальных заданий.

вариант-3

Кол-во баллов: 9

Реализуйте ССА-КЕМ на базе криптосистемы Мак–Элиса (*добавляемая ошибка генерируется псевдослучайно на основе сообщения t ; при декодировании проверяется, что ошибка сгенерирована верно*).

вариант-4

Кол-во баллов: 14

Реализуйте алгоритм Ли–Брикелля для синдромного декодирования случайных линейных кодов ($He^T = s, wt(e) \leq t$).

вариант-5

Кол-во баллов: 12

Реализуйте этап восстановления $\alpha = (\alpha_1, \dots, \alpha_n)$ для кода $GRS(\alpha, \beta)$ из атаки Сидельникова–Шестакова.

вариант-6

Кол-во баллов: 12

Реализуйте алгоритм цифровой подписи LESS (*параметры: $q = 31, n = 171, k = 91, \omega = 128$*) и проверьте корректность его работы.

- **Генерация ключей:** пусть $G \in \mathbb{F}_q^{k \times n}$ — случайная матрица ранга k , $S \in \mathbb{F}_q^{k \times k}$ — случайная обратимая $(k \times k)$ -матрица, $P \in \mathbb{F}_q^{n \times n}$ — случайная перестановочная матрица. Тогда $(G, \tilde{G} = S \cdot G \cdot P)$ — публичный ключ (*ключ проверки подписи*), P — секретный ключ (*ключ создания подписи*).
- **Создание подписи:** для подписи сообщения m необходимо сгенерировать ω обратимых $n \times n$ -матриц Q_i и вычислить

$$c = \text{Hash}(\text{rref}(G \cdot Q_1), \dots, \text{rref}(G \cdot Q_\omega)),$$

где rref — функция, вычисляющая приведённый ступенчатый вид матрицы (в SageMath: $\text{rref}()$). Далее необходимо вычислить вектор $\mathbf{b} = (b_1, \dots, b_\omega) \in \mathbb{F}_2^\omega$:

$$(b_1, \dots, b_\omega) = \text{Hash}(c, m)$$

и набор матриц

$$R_i = \begin{cases} Q_i, & b_i = 0 \\ P^{-1}Q_i, & b_i = 1 \end{cases}$$

тогда $(c, \mathbf{b}, R_1, \dots, R_\omega)$ — цифровая подпись сообщения m .

- **Проверка подписи:**

1. проверить, что $\mathbf{b} = \text{Hash}(c, m)$;
2. вычислить матрицы

$$U_i = \begin{cases} GR_i, & b_i = 0 \\ \tilde{G}R_i, & b_i = 1 \end{cases}$$

и проверить равенство $c = \text{Hash}(\text{rref}(U_1), \dots, \text{rref}(U_\omega))$.

вариант-7

Кол-во баллов: 14

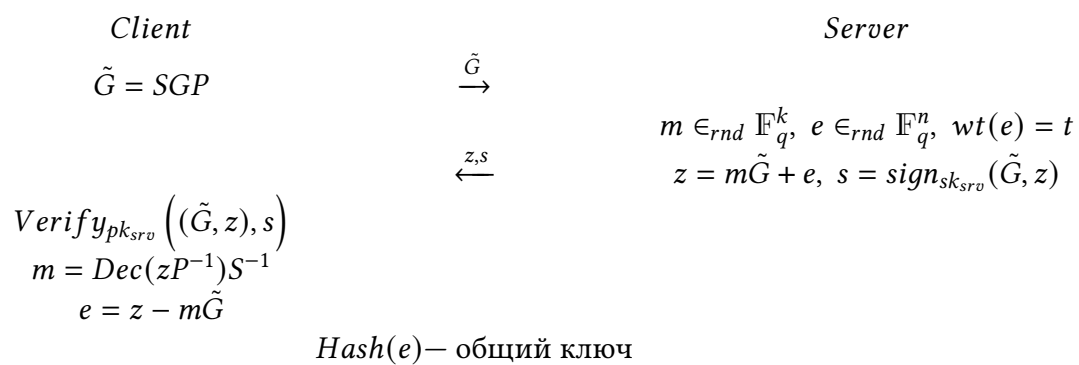
Реализуйте схему подписи UOV (параметры $q = 3$, $n = 20$, $k = 10$, $\tau = 10$).

вариант-8

Кол-во баллов: 14 (индивидуально), 10 (в группе до 3 человек)

Реализуйте протокол рукопожатия из TLS на основе криптосистемы Мак-Элиса и подписи

LESS или UOV:



Публичный ключ проверки подписи сервера pk_{srv} считается общеизвестным.