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 конгуэртным генератором псевдослучайных чисел (аффинным генератором).

вариант-2

Кол-во баллов: 7
Реализуйте CPA-KEM 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 CCA-KEM на базе криптосистемы Мак–Элиса *(добавляемая ошибка генерируется псевдослучайно на основе сообщения m; 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 $\alpha = (\alpha_1, \ldots, \alpha_n)$ 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

$$c = Hash\left(rref(G \cdot Q_1), \ldots, rref(G \cdot Q_\omega)\right),$$

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

$$(b_1, \ldots, b_\omega) = Hash(c, m)$$

и набор матриц

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

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

- **Проверка подписи:**

  1. проверить, что $\mathbf{b} = Hash(c, m)$;
  2. вычислить матрицы
  $$U_i = \begin{cases} GR_i, & b_i = 0 \\ \tilde{G}R_i, & b_i = 1 \end{cases}$$
  и проверить равенство $c = Hash(rref(U_1), \ldots, rref(U_\omega))$.

вариант-7

Кол-во баллов: 14
Реализуйте схему подписи UOV *(параметры $q = 3$, $n = 20$, $k = 10$, $\tau = 10$)*.

- **Генерация ключа.** В первую очередь необходимо сгенирировать разрешимую систему из k однородных квадратичных уравнений от n неизвестных над полем $\mathbb{F}_q$ следующего вида

$$F(x_1, \ldots, x_n) = \begin{cases} f^{(1)}(x_1, \ldots, x_n), \\ \ldots \\ f^{(k)}(x_1, \ldots, x_n). \end{cases}, \quad f^{(i)}(x_1, \ldots, x_n) = \sum_{j=1}^{\tau} \sum_{t=j}^{\tau} f_{j,t}^{(i)} x_j x_t + \sum_{j=1}^{\tau} \sum_{t=\tau+1}^{n} f_{j,t}^{(i)} x_j x_t.$$

Нетрудно заметить, что в силу того, что переменные с номерами $\geq \tau + 1$ между собой не перемножаются, система $F(x_1, \ldots, x_n) = (b_1, \ldots, b_m)$ может быть легко решена (см. создание подписи). Далее, сгенерированную систему необходимо замаскировать под случайную: для этого генерируется случайная обратимая $(n \times n)$–матрица S и в систему F делается подстановка

$$(x_1, \ldots, x_n) = (y_1, \ldots, y_n) \cdot S$$

(т.е. переменные x_j в системе заменяются какими-то линейными комбинациями новых переменных y_j). Результирующая система

$$\tilde{F}(y_1, \ldots, y_n) = F\left((y_1, \ldots y_n) \cdot S\right)$$

является публичным ключом *(ключом проверки подписи).*

- **Создание подписи.** Предположим, что необходимо подписать некоторое сообщение m, для этого вычисляется $Hash(m)$ и переводится в q-ичную систему счисления:

  $$Hash(m) = b_1 q^0 + b_2 q^1 + b_3 q^2 + \cdots + b^k q^{k+1} + \ldots,$$

  откуда находится вектор $\overline{b} = (b_1, \ldots, b_k) \in \mathbb{F}_q^k$. Далее необходимо решить систему

  $$F(x_1, \ldots, x_n) = (b_1, \ldots, b_k),$$

  что можно сделать в 2 шага:

  1. сгенерировать случайный вектор $(a_1, \ldots, a_\tau) \in \mathbb{F}_q^\tau$ и подставить в предыдущее уравнение вместо первых τ неизвестных:

  $$F(a_1, \ldots, a_\tau, x_{\tau+1}, \ldots, x_n) = \begin{cases} \underbrace{\sum_{j=1}^{\tau} \sum_{t=j}^{\tau} f_{j,t}^{(1)} a_j a_t}_{\text{константа}} + \underbrace{\sum_{j=1}^{\tau} \sum_{t=\tau+1}^{n} f_{j,t}^{(1)} a_j x_t}_{\text{линейное уравнение}} \\ \ldots \\ \underbrace{\sum_{j=1}^{\tau} \sum_{t=j}^{\tau} f_{j,t}^{(k)} a_j a_t}_{\text{константа}} + \underbrace{\sum_{j=1}^{\tau} \sum_{t=\tau+1}^{n} f_{j,t}^{(k)} a_j x_t}_{\text{линейное уравнение}} \end{cases} = \begin{pmatrix} b_1 \\ b_2 \\ \ldots \\ b_{k-1} \\ b_k \end{pmatrix}$$

  2. решить полученную на прошлом шаге линейную систему. Если система оказалась неразрешимой, то перегенерировать $(a_1, \ldots, a_\tau)$.

  Пусть $(a_1, \ldots, a_n)$ — решение системы $F(x_1, \ldots, x_n) = (b_1, \ldots, b_k)$, тогда $u = (a_1, \ldots, a_n) \cdot S^{-1}$ — подпись сообщения.

- **Проверка подписи.** По сообщению m необходимо найти вектор $(b_1, \ldots, b_k)$ и проверить, что $\tilde{F}(u) = (b_1, \ldots, b_k)$.

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:

$$
\begin{array}{ccc}
Client & & Server \\
\tilde{G} = SGP & \xrightarrow{\tilde{G}} & \\
 & & m \in_{rnd} \mathbb{F}_q^k,\ e \in_{rnd} \mathbb{F}_q^n,\ wt(e) = t \\
 & \xleftarrow{z,s} & z = m\tilde{G} + e,\ s = sign_{sk_{srv}}(\tilde{G}, z) \\
Verify_{pk_{srv}}\left((\tilde{G}, z), s\right) & & \\
m = Dec(zP^{-1})S^{-1} & & \\
e = z - m\tilde{G} & & \\
 & Hash(e) \text{— общий ключ} &
\end{array}
$$

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