15 Задачи коллоквиума по криптографии

Криптосистема на задаче о рюкзаке

15.1 Пусть для передачи информации используется криптосистема, основанная на задаче о рюкзаке. Часть Вашего секретного ключа составляют супервозрастающий вектор $a' = (1, 2, 4, 9, 17, 34)$, число $m = 69$ и число $\omega = 31$. Каждая буква русского алфавита (без буквы "ё") кодируется двоичным набором длины 6, соответствующим порядковому номеру буквы (буква "а" имеет номер 1). Считаем, что первый бит в наборе является старшим. Используя открытый ключ каждой букве сопоставляется некоторое целое число.

а) Найти открытый и полный секретный ключи.

б) Дешифровать сообщение $x = 62, 19, 81, 121, 58, 180$. Определить переданное слово.

Ответ 15.1 а) Открытый ключ $a = (31, 62, 55, 3, 44, 19)$.

Полный секретный ключ $a' = (1, 2, 4, 9, 17, 34)$, $m = 69$, $\omega = 31$, $\omega^{-1} = 49$.

б) После преобразования с помощью секретного ключа получается сообщение $y = 2, 34, 36, 64, 13, 57$, переданное слово есть "ПАРОЛЬ".

15.2 Пусть для передачи информации используется криптосистема, основанная на задаче о рюкзаке. Часть Вашего секретного ключа составляют супервозрастающий вектор $a' = (3, 5, 9, 19, 45)$, число $m = 100$ и число $\omega = 21$. Каждая буква русского алфавита (без буквы "ё") кодируется двоичным набором длины 5, соответствующим порядковому номеру буквы (буква "а" имеет номер 0). Считаем, что первый бит в наборе является старшим. Используя открытый ключ каждой букве сопоставляется некоторое целое число.

а) Найти открытый и полный секретный ключи.

б) Дешифровать сообщение $x = 193, 104, 162, 301, 45, 63, 167$. Определить переданное слово.

Ответ 15.2 а) Открытый ключ $a = (63, 5, 89, 99, 45)$.

Полный секретный ключ $a' = (3, 5, 9, 19, 45)$, $m = 100$, $\omega = 21$, $\omega^{-1} = 81$.

б) После преобразования с помощью секретного ключа получается сообщение $y = 33, 24, 22, 81, 45, 3, 27$, переданное слово есть "ОКТЯБРЬ".

Криптосистема Мак-Элиса

15.3 Пусть для передачи информации используется криптосистема Мак-Элиса. Ваш секретный ключ составляют: невырожденная матрица S, порождающая матрица G:

$$S = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}, G = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

и матрица P, соответствующая подстановке $\pi = (142536)$. Секретная информация кодируется с помощью открытого ключа двоичными блоками длины 3. Каждый блок представляет собой двоичную запись некоторого целого числа от 0 до 7.

а) Найти открытый ключ криптосистемы.

б) Дешифровать полученное сообщение $x = (101100)$ и восстановить секретную информацию.

Ответ 15.3 а) Открытый ключ матрица

$$G' = \begin{pmatrix} 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 \end{pmatrix}.$$

б) Было передано сообщение "5", представленное вектором (101). При передаче использовался вектор ошибок $e = (000001)$.

15.4 Пусть для передачи информации используется криптосистема Мак-Элиса. Ваш секретный ключ составляют: невырожденная матрица S, порождающая матрица G:

$$S = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{pmatrix}, G = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}$$

и матрица P, соответствующая подстановке $\pi = (634512)$. Секретная информация кодируется с помощью открытого ключа двоичными блоками длины 3. Каждый блок представляет собой двоичную запись некоторого целого числа от 0 до 7.

а) Найти открытый ключ криптосистемы.

б) Дешифровать полученное сообщение $x = (011110)$ и восстановить секретную информацию.

Ответ 15.4 а) Открытый ключ матрица

$$G' = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

б) Было передано сообщение "7", представленное вектором (111). При передаче использовался вектор ошибок $e = (001000)$.

Электронная подпись

15.5 Пусть банкир В. выбирает простые числа 3 и 5. Вкладчик А. выбирает 7 и 11. $K_{B.,open} = \{15, 7\}$, $K_{A.,open} = \{77, 7\}$. Как с помощью RSA вкладчик А. может передать В. свое секретное поручение $m = 13$?

Ответ 15.5 Поручение А.: 13, подпись - 7.

15.6 Пусть банкир В. выбирает простые числа 11 и 2. Вкладчик А. выбирает 3 и 5. $K_{B.,open} = \{15, 7\}$, $K_{A.,open} = \{22, 3\}$. Как с помощью RSA вкладчик А. может передать В. свое секретное поручение $m = 13$?

Ответ 15.6 Поручение А.: 3, подпись - 48.

Криптосистема RSA

15.7 Для получения секретной информации используется криптосистема RSA. Выбрав два простых числа p и q, Алиса формирует число $n = p \cdot q$ и выбирает e взаимно простым с числом $\varphi(n)$. Затем она публикует пару $\{n, e\}$ в газете "Университетская жизнь". Используя открытый ключ, передать Алисе секретное сообщение m. Дешифровать его с помощью секретного ключа.

а) $p = 13$, $q = 19$, $e = 11$, $m = 5$;

б) $p = 3$, $q = 11$, $e = 3$, $m = 15$.

Ответ 15.7 а) открытое сообщение y=177.
б) открытое сообщение y=9.

Криптосистема Шамира

15.8 Пусть открытый ключ $K = \{p = 23\}$. Каким образом A. секретно может передать B. важное сообщение $m = 10$? Пусть $K_{A_{priv}} = \{7\}$, $K_{B_{priv}} = \{5\}$.

Открытое распределение ключей Диффи и Хэллмена

15.9 Пусть открытый ключ $\{GF(3^3), \alpha\}$,где α корень примитивного многочлена $f(x)$. Используя открытое распределение ключей Диффи и Хэллмена, получить общий секретный ключ, если A. задумала число 7, а B. - число 5.

а) $f(x) = x^3 + x^2 - 1$;
б) $f(x) = x^3 - x^2 + 1$.