УДК 513.6:517.1:519.48

ПРОТОКОЛ ФОРМИРОВАНИЯ СЕКРЕТНЫХ КЛЮЧЕЙ ШИФРОВАНИЯ АБОНЕНТАМИ ОТКРЫТЫХ КАНАЛОВ СВЯЗИ НА ОСНОВЕ ОБОБЩЕННЫХ МАТРИЦ ГАЛУА

Анатолий Белецкий

В статье рассмотрены методы формирования секретных ключей шифрования двумя абонентами открытых коммуникационных сетей. В генерации ключа принимают участия оба абонента сети. В основу протокола обмена ключами положены алгоритмы ассиметричной (двухключевой) криптографии. Решение проблемы синтеза ключей предполагает вычисление однонаправленных функций и базируется на использовании обобщенных подобных матриц Галуа. В качестве матриц преобразования подобия выбраны перестановочные матрицы. Для матриц Галуа разработан простой способ их построения, названный методом диагонального заполнения. Обобщенные матрицы Галуа связаны отношением изоморфизма с образующими их элементами и зависят от выбранных неприводимых полиномов, порождающих матрицы. Обсуждаются варианты способов построения оперативной смены ключей шифрования в каждом сеансе связи наземных пунктов управления с беспилотными летательными аппаратами.

Ключевые слова: *протокол обмена ключами, однонаправленные функции, обобщенные матрицы Галуа, подобные матрицы, расширенные поля Галуа, отношение изоморфизма.*

I. Введение и постановка задачи. Одной из наиболее актуальных проблем современной криптографии является формирование секретных ключей шифрования легализованными абонентами открытых компьютерных сетей или иных открытых каналов передачи информации. Особую остроту приобретает данная проблема в системах управления беспилотными летательными аппаратами (БПЛА), поскольку несанкционированный доступ, например, в радиоканал приема-передачи командно-телеметрической информации сопряжен с риском потери аппарата или может привести к другим тяжким последствиям [1].

Для обмена зашифрованными сообщениями между двумя абонентами криптосистемы необходимо, чтобы обоим участникам обмена доставлялись сохраняемые в секрете ключи шифрования. Технология формирования секретных ключей по открытым каналам связи в случае, когда каждый из двух абонентов сети участвует в генерации этого секретного ключа, носит название *протокола обмена ключами* (ПрОК), являющегося частным случаем *протокола распределения ключей*. Вторым типом протокола предполагается не только выработка секретного ключа шифрования, но и его распределение между всеми абонентами (число которых может превышать два) некоторой легализованной группы открытой коммуникационной сети. И, наконец, в том случае, когда секретный ключ не вырабатывается в протоколе, а приобретается заранее кем-либо из участников группы, то такой протокол носит название *протокола распространения ключей* [2, 3]. Предметом исследования в данной статье являются исключительно протоколы первого типа, то есть протоколы обмена ключами.

Проблема обмена секретными ключами шифрования решается, как правило, с помощью двухключевой (асимметричной) криптографии. При таком её решении используется некий алгоритм, опирающийся на так называемые *односторонние* (*однонаправленные*) функции. Вычисление односторонних функций в одном направлении не представляет особых затруднений, тогда как нахождение обратной функции требует значительных вычислительных ресурсов. В частности, стойкость криптографических систем RSA, популярном алгоритме, часто применяемом для построения односторонних функций и протоколов обмена ключами, основывается на факторизации больших чисел и требует экпоненциального по числу знаков факторизуемого числа операций [4].

Главный недостаток RSA-протоколов, ограничивающий их применение в *системах оперативной смены ключей шифрования*, состоит в их низком быстродействии, обусловленном необходимостью выполнения вычислений над двоичными операндами большой размерности, достигающих нескольких Кбит. Альтернативой RSA-протоколам могут служить матричные ПрОК, один из возможных вариантов которых строится на односторонней функции Мегрелишвили [5]. Особенность алгоритма Мегрелишвили состоит в том, что используемая в нем матрица преобразования является матрицей нечетного порядка, что может создавать определенные затруднения в криптографических приложениях.

В связи с вышеизложенным проблема разработки эффективных протоколов обмена ключами шифрования продолжает оставаться актуальной.

В данной статье разрабатываются способы формирования односторонних функций, бази-

рующийся на так называемых *обобщенных матрицах Галуа* (ОМГ), и предлагаются на их основе алгоритмы построения ОМГ-ПрОК, ориентированные на применение в системах оперативной смены ключей шифрования в каждом сеансе связи между наземным пунктом управления (НПУ) и бортовой аппаратурой БПЛА. Под *сеансом связи* понимается передача по радиоканалу одиночного пакета информации в направлении НПУ – борт БПЛА или наоборот.

II. Классические матрицы Галуа. Термин *матрицы Галуа*, как и биективно связанные с ними *матрицы Фибоначчи*, заимствованы из теории помехоустойчивого кодирования и криптографии, в которых широко применяются генераторы бинарных псевдослучайных последовательностей (ПСП) в конфигурациях Галуа и Фибоначчи, построенные на линейных регистрах сдвига (ЛРС) с линейными обратными связями (ЛОС) [6]. Известно, что для того чтобы ЛРС являлся генератором ПСП максимального периода, соответствующий полином обратной связи должен быть *примитивным полиномом* (ПрП). Пример генератора Галуа восьмого порядка, формирующего ПСП максимального периода, показан на рис. 1.

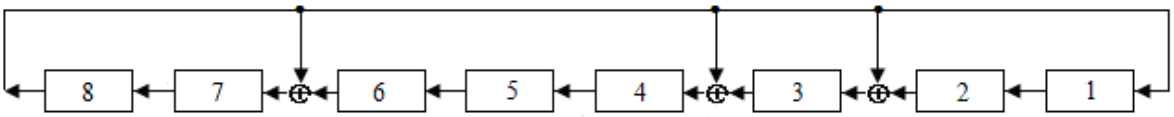

Рис. 1. Структурная схема генератора ПСП по схеме Галуа над ПрП $f_8 = 101001101$

Классический генератор Галуа, представленный на рис. 1, сопоставляет каждому ненулевому элементу поля $GF(2^8)$ соответствующую степень примитивного элемента $\omega = 10$ по модулю ПрП $f_8 = 101001101$. В качестве элементов памяти линейных регистров используются, как правило, $D-$ триггеры, уровень сигнала на выходе которых (0 или 1) после подачи синхроимпульса повторяет уровень сигнала, подведенного к входу триггера. Блок $\oplus$ в ЛРС осуществляет операцию сложения по модулю 2 (операцию XOR).

Как следует из структурной схемы генератора (рис. 1) обратные связи в классических генераторах (регистрах) Галуа однозначно определяются выбранным ПрП f_n степени n и формируются таким способом: отклики каждого разряда ($D-$ триггера) ЛРС поступают на входы последующих разрядов, являясь для них функциями возбуждения. Кроме того, отклик старшего разряда регистра подается (по схеме XOR) на входы тех и только тех разрядов, номера которых совпадают с номерами ненулевых мономов ПрП. При этом младшему моному, расположенному справа полинома f_n, как и младшему (правому) разряду регистра на рис. 1, соответствует номер 1.

Двоичные ПрП f_n порождают поля $GF(2^n)$, минимальный примитивный элемент которых равен 10. Последовательность степеней любого примитивного элемента θ поля Галуа по модулю ПрП f_n, то есть $\theta^k \pmod{f_n}$, $k = 0,1,\ldots$ формируют последовательность максимальной длины ($m-$последовательность). Фрагмент такой последовательности для полинома $f_8 = 101001101$ представлен в табл. 1.

Непосредственной проверкой легко убедиться в том, что ЛРС (рис. 1) с обратными связями, образуемыми ПрП f_8, порождает последовательность состояний регистра, совпадающую с $m-$последовательностью (табл. 1).

Таблица 1

Фрагмент последовательности степеней элемента $\theta = 10$ по модулю $f_8 = 101001101$

k	8	7	6	5	4	3	2	1
0	0	0	0	0	0	0	0	1
1	0	0	0	0	0	0	1	0
2	0	0	0	0	0	1	0	0
3	0	0	0	0	1	0	0	0
4	0	0	0	1	0	0	0	0
5	0	0	1	0	0	0	0	0
6	0	1	0	0	0	0	0	0
7	1	0	0	0	0	0	0	0
8	0	1	0	0	1	1	0	1
9	1	0	0	1	1	0	1	0
10	0	1	1	1	1	0	0	1
…	…	…	…	…	…	…	…	…
254	0	0	0	0	0	0	0	1

Каждый линейный ЛРСЛОС-генератор ПСП максимального периода, может быть представлен эквивалентной ему примитивной матрицей Галуа, формирующей ту же самую $m-$последовательность, что и генератор ПСП.

Обозначим через $G_f^{(n)}$ двумерную матрицу Галуа $n-$го порядка над неприводимым полиномом (НП) f_n. С помощью $G_f^{(n)}$ введем рекур-

рентное вычисление состояний $S(t)$ регистра в дискретные моменты времени t:

$$S(t) = S(t-1)\cdot G_f^{(n)}, \quad t = 1, 2, \ldots$$
$$S(0) = 00000001. \qquad (1)$$

Вектором $S(0)$ выделяется нижняя строка (припишем ей номер 1) матрицы $G_f^{(n)}$. Следовательно, в нижней строке матрицы $G_f^{(8)}$ необходимо записать (согласно табл. 1) значение $S(1)=10$, совпадающее с минимальным образующим элементом (ОЭ) $\omega = 10$ поля $GF(2^8)$ над ПрП $f_8 = 101001101$. Соотношением $S(2) = S(1)\cdot G_f^{(8)}$ выделяется вторая (снизу) строка матрицы $G_f^{(n)}$, которая, по данным табл. 1, должна быть равна 100. Продолжая вычисления таким способом, приходим к матрице

$$G_f^{(8)} = \begin{bmatrix} 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix} \begin{matrix} 8 \\ 7 \\ 6 \\ 5 \\ 4 \\ 3 \\ 2 \\ 1 \end{matrix}. \qquad (2)$$
$$8\ 7\ 6\ 5\ 4\ 3\ 2\ 1$$

В соответствии с (2) алгоритм синтеза классических матриц Галуа может быть сформулирован следующим образом. Пусть f_n – векторная форма примитивного полинома степени n такая, что $f_n = \{1, u_{n-1}, u_{n-2}, ..., u_2, u_1, 1\}$, $u_i \in \{0,1\}$, $i = \overline{1, n-1}$, и $\omega = 10$ – минимальный ОЭ поля $GF(2^n)$, порождаемого ПрП f_n. Поместим образующий элемент 10 справа в нижней строке матрицы Галуа и заполним элементы матрицы, придерживаясь простого правила. Поставим единицы в элементах диагонали, расположенной ниже главной диагонали матрицы, а в оставшихся элементах матрицы $G_f^{(n)}$, кроме верхней строки, запишем нули. В верхней $(n-й)$ строке матрицы Галуа следует ожидать появления $(n+1)-$битного вектора 100…0. Но это недопустимо, так как порядок матрицы равен n. Приведя $(n+1)-$битный вектор к остатку по модулю f_n, приходим к заключению, что в верхней строке матрицы $G_f^{(n)}$ следует разместить ПрП f_n, исключая его старшую единицу, т.е. $n-$битный вектор $u_{n-1}, u_{n-2}, ..., u_2, u_1, 1$.

На основании предложенного метода, назовем его *методом диагонального заполнения*, получим общую форму классической матрицы Галуа $n-$го порядка, которая имеет вид:

$$G_f^{(n)} = \begin{pmatrix} u_{n-1} & u_{n-2} & \cdots & u_2 & u_1 & 1 \\ 1 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 1 & 0 & 0 \\ 0 & 0 & \cdots & 0 & 1 & 0 \end{pmatrix}. \qquad (3)$$

Матрицы $G_f^{(n)}$ над ПрП f взаимно однозначно (биективно) связаны с матрицами Фибоначчи $F_f^{(n)}$ оператором $\perp$ *правостороннего транспонирования* [7], то есть транспонирования относительно вспомогательной диагонали,

$$F_f^{(n)} \xleftrightarrow{\perp} G_f^{(n)}.$$

Поэтому ограничимся в дальнейшем рассмотрением только лишь матриц Галуа.

III. Обобщенные матрицы Галуа. Введем

Определение ОМГ. *Обобщенными будем называть матрицы Галуа $G_{f,\omega}^{(n)}$, образующий элемент которых ω совсем не обязательно является примитивным элементом поля $GF(p^n)$, порождаемого произвольным неприводимым полиномом f_n степени n.*

Синтез обобщенных матриц Галуа $G_{f,\omega}^{(n)}$ осуществляется выше введенным методом диагонального заполнения и сводится к таким действиям. В нижней строке синтезируемой ОМГ записывается образующий ее элемент $\omega \geq 10$, являющийся элементом поля $GF(p^n)$ над НП f_n. Разряды строки, расположенные слева от ω, заполняются нулями. Последующие строки матрицы (снизу вверх) образуются сдвигом предыдущей строки на один разряд влево, а в освобождающийся правый разряд заносится 0. Если при сдвиге старший ненулевой разряд строки выходит за пределы матрицы, то векторы, отвечающие таким строкам, приводятся к остатку по модулю f_n и, тем самым, строка вновь становится n разрядной.

Из теории полиномов одной переменной x известно, что умножение произвольного полинома $\omega_k(x)$ степени k на x эквивалентно его сдвигу на один разряд влево и, соответственно, увеличению на 1 степени полинома [5]. Или, другими словами,

$$x \cdot \omega_k(x) \to \omega_{k+1}(x). \quad (4)$$

Воспользовавшись соотношением (4) и, принимая во внимание способ формирования ОМГ, запишем цепочку преобразований:

$$G_{f,\omega}^{(n)} \Rightarrow \begin{pmatrix} x^{n-1}\cdot\omega \\ x^{n-2}\cdot\omega \\ \vdots \\ x\cdot\omega \\ 1 \end{pmatrix} \bmod f_n = \omega \cdot \begin{pmatrix} x^{n-1} \\ x^{n-2} \\ \vdots \\ x \\ 1 \end{pmatrix} \bmod f_n. \quad (5)$$

Элементами правого вектор-столбца в соотношении (5) являются мономы, которые, будучи представленными в двоичной форме, обращают вектор-столбец в единичную матрицу E, то есть

$$\begin{pmatrix} x^{n-1} \\ x^{n-2} \\ \vdots \\ x \\ 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & \cdots & 0 & 1 \end{pmatrix} = E,$$

что позволяет сформулировать следующее утверждение.

Утверждение. *Обобщенная матрица Галуа* $G_{f,\omega}^{(n)}$ *порядка* n *над неприводимым полиномом* f_n *изоморфна ее образующему элементу* ω*, являющемуся элементом поля* $GF(p^n)$ *характеристики* p

$$G_{f,\omega}^{(n)} \leftrightarrow \omega. \quad (6)$$

Следовательно, между ОМГ $G_{f,\omega}^{(n)}$ и ее образующим элементом ω существует взаимно однозначное соответствие (изоморфизм), отображаемое отношением (6). Кроме того, легко установить, что изоморфизм (6) приводит к таким последствиям.

Следствие 1. Для того чтобы возвести матрицу $G_{f,\omega}^{(n)}$ в степень k достаточно вычислить образующий элемент $\omega_k = \omega^k (\bmod f_n)$ и по методу диагонального заполнения составить матрицу $G_{f,\omega_k}^{(n)}$.

Следствие 2. Минимальное ненулевое значение степени e, обеспечивающее равенство $(G_{f,\omega}^{(n)})^e = E$, совпадает с порядком ord элемента ω, образующего матрицу $G_{f,\omega}^{(n)}$.

Следствие 3. Обобщенная матрица Галуа $G_{f,\omega}^{(n)}$ примитивна, если примитивным является образующий её элемент ω, то есть если $\omega = \theta$.

Следствие 4. Матрицы $G_{f,\omega_1}^{(n)}$ и $G_{f,\omega_2}^{(n)}$, $\omega_1 \neq \omega_2$, коммутативны, поскольку являются элементами одной и той же мультипликативной группы максимального порядка GF^*, составленной из степеней матрицы $G_{f,\theta}^{(n)}$, произвольный образующий примитивный элемент которой θ принадлежит полю $GF(p^n)$ над НП f_n.

Множество ОМГ может быть расширено за счет введения *подобных матриц Галуа* ${}^*G_{f,\omega}^{(n)}$, определяемых соотношением

$${}^*G_{f,\omega}^{(n)} = P^{-1} \cdot G_{f,\omega}^{(n)} \cdot P,$$

где P – матрица преобразования подобия. В качестве P – матриц выбраны перестановочные матрицы n – го порядка, для которых $P^{-1} = P^T$.

В отличие от исходных ОМГ $G_{f,\omega}^{(n)}$ матрицы ${}^*G_{f,\omega}^{(n)}$, оставаясь коммутативными, утрачивают свойство изоморфизма. Данная особенность подобных матриц Галуа как раз и обеспечивает возможность построения *односторонних функций*, используемых в предлагаемых протоколах обмена ключами абонентами открытых коммуникационных каналов передачи информации.

IV. ОМГ-протокол обмена ключами шифрования. Введем неформальное определение односторонней функции [8].

Определение. *Функция* $f : X -> Y$ *называется односторонней (однонаправленной), если* $f(x)$ *может быть легко вычислена для каждого* $x \in X$*, тогда как почти для всех* $y \in Y$ *вычисление такого* $x \in X$*, что* $f(x) = y$ *(при условии, что хотя бы один такой* x *существует), является сложным.*

Ниже приведены краткие пояснения к предлагаемому ОМГ-протоколу обмена ключами в открытых коммуникационных сетях. Протоколом предполагается формирование абонентами сети новой односторонней функции, посредством которой и вычисляется общий секретный ключ шифрования.

В качестве *открытого ключа* протокола приняты: вектор инициализации V, являющийся $n-$битным вектором; неприводимый двоичный полином f_n степени n и перестановочная матрица P $n-$го порядка. Каждый из абонентов сети A и B вырабатывает *секретные* $n-$*битные ключи* ω_α и ω_β соответственно. Общий секретный ключ K определяется в результате выполнения абонентами таких двух этапов вычислений:

Этап 1. Абонент A генерирует случайный вектор ω_α, находит сначала ОМГ $G^{(n)}_{f,\omega}$, затем подобную матрицу ${}^*G^{(n)}_{f,\omega}$, вычисляет вектор $V_\alpha = V \cdot {}^*G^{(n)}_{f,\omega_\alpha}$ и направляет его абоненту B.

Аналогичные операции осуществляет абонент B, определяя вектор $V_\beta = V \cdot {}^*G^{(n)}_{f,\omega_\beta}$, который направляет абоненту A.

Векторы V_α и V_β как раз и являются односторонними функциями, которые построены на основе подобных ОМГ.

Этап 2. Абонент A умножает принятый от абонента B вектор $V_\beta = V \cdot {}^*G^{(n)}_{f,\omega_\beta}$ на свою секретную матрицу ${}^*G^{(n)}_{f,\omega_\alpha}$, формируя ключ

$$K_\alpha = V_\beta \cdot {}^*G^{(n)}_{f,\omega_\alpha} = V \cdot {}^*G^{(n)}_{f,\omega_\beta} \cdot {}^*G^{(n)}_{f,\omega_\alpha} =$$
$$= V \cdot (P^{-1} \cdot G^{(n)}_{f,\omega_\beta} \cdot P) \cdot (P^{-1} \cdot G^{(n)}_{f,\omega_\alpha} \cdot P) =$$
$$= V \cdot (P^{-1} \cdot G^{(n)}_{f,\omega_\beta} \cdot G^{(n)}_{f,\omega_\alpha} \cdot P).$$

Точно такие же вычисления выполняет абонент B, извлекая вектор

$$K_\beta = V \cdot (P^{-1} \cdot G^{(n)}_{f,\omega_\alpha} \cdot G^{(n)}_{f,\omega_\beta} \cdot P).$$

Поскольку ОМГ $G^{(n)}_{f,\omega_\alpha}$ и $G^{(n)}_{f,\omega_\beta}$ коммутативны, то оказывается, что $K_\alpha = K_\beta = K$ и, следовательно, оба абонента сети получают одинаковый секретный ключ шифрования K.

Если же вместо подобных матриц ${}^*G^{(n)}_{f,\omega}$ использовать обычные ОМГ $G^{(n)}_{f,\omega}$, то в силу их изоморфизма (3) противник, перехватив векторы V_α и V_β, может вычислить секретные ключи ω_α и ω_β, так как в общем случае

$$V_\gamma = V \cdot G^{(n)}_{f,\omega_\gamma} = V \cdot \omega_\gamma (\mathrm{mod}\, f_n),$$
$$\gamma = \alpha \text{ или } \beta. \qquad (4)$$

Ввиду того, что V и f_n – известные величины, противник, разрешая равенства (4) относительно ω_γ, вычисляет секретные ключи ω_α и ω_β, что и приводит к взлому общего секретного ключа K.

И в заключение раздела отметим, что предлагаемый ОМГ-протокол, как и классический протокол Диффи-Хеллмана, а также ближайший аналог ОМГ-протокола – матричный протокол Мегрелишвили, не защищен от атаки типа «человек посередине», что, однако, не снижает достоинств разработанного протокола, среди которых отметим, прежде всего, возможность его применения в системах оперативной смены ключей шифрования.

Выводы. В статье разработаны простые алгоритмы синтеза обобщенных матриц Галуа, которым присущи такие основные особенности. Во-первых, ОМГ могут быть построены для произвольных НП, тогда как классические матрицы Галуа определяются лишь над примитивными полиномами. Во-вторых, каждому ПрП отвечает единственная примитивная матрица Галуа, тогда как для каждого НП число примитивных ОМГ совпадает с числом примитивных элементов θ расширенного поля $GF(2^n)$, порождаемого выбранным неприводимым полиномом f_n.

Установленное в работе отношение изоморфизма, существующее между ОМГ и образующими их элементами, открывает перспективу построения пространственных матриц Галуа и разработку теоретических основ алгебры пространственных обобщенных матриц Галуа, что и может составить направление дальнейших исследований, начало которому закладывается данной работой.

ЛИТЕРАТУРА

[1]. Иран объявил о захвате американского беспилотника. / http://zn.ua

[2]. Ивонин М. В. Криптографические протоколы распределения ключей для групп с динамическим составом участников. / www.itsecure.org.ua

[3]. Введение в криптографию: новые математические дисциплины. Учебник/ под ред. В.В. Ященко. – СПб: Питер, 2001. – 287 с.

[4]. Коутинхо С. Введение в теорию чисел. Алгоритм RSA. / С. Коухтиньо. — Постмаркет, 2007. – 328 с.

[5]. Megrelishvili R. Investigation of new matrix-key function for the public cryptosystems. / R. Megrelishvili, M. Chelidze, G. Besiashvili. The Third International Conference “Problems of cybernetics and Information”, Volume 1, September 6-8, Baku,

Azerbaijan, Section N1, "Information and Communication Technologies", 2010, pp. 75-78.
[6]. Поточные шифры. Результаты зарубежной открытой криптологии. – М., 1997. / [Электронный ресурс]. – Режим доступа: ttp//www/ ssl/stu/neva/ru/psw/crypto/potok/st r_ciph.htm
[7]. Муллажонов Р. В. Обобщенное транспонирование матриц и структуры линейных крупномасштабных систем. / Р. В. Муллажонов // Доповіді НАНУ, 2009, № 10. С. 27-35.
[8]. Однонаправленные функции. / http: // crypto. pp. ua/2010/06/odnonapravlennye- funkcii/
[9]. Лидл Р. Конечные поля. Монография в 2-х томах. / Р. Лидл, Г. Нидеррайтер. Т. 1. – М.: Мир, 1988. – 432 с.

REFERENCES

[1]. Iran announced the capture of the American drone. / http://zn.ua
[2]. M. Ivonin. Cryptographic key distribution protocols for groups with dynamic composition of participants. / www.itsecure.org.ua
[3]. Introduction to cryptography: new mathematical discipline. Textbook, Ed. V.V. Yaschenko, SPb.: Piter, 2001, 287 p.
[4]. C. Koutinho. Introduction to the theory of numbers. The algorithm is RSA, Postmarket, 2007, 328 p.
[5]. R. Megrelishvili, M. Chelidze, G. Besiashvili. The Third International Conference "Problems of cybernetics and Information", Volume 1, Sept. 6-8, Baku, Azerbaijan, Section N1, "Information and Communication Technologies", 2010, pp. 75-78.
[6]. Stream Ciphers. The results of the open foreign cryptology, M., 1997. http//www/ssl/stu /neva/ ru/psw/crypto/ potok/str_ciph.htm
[7]. R. Mullajonov. Generalized transposition of matrices and linear structure of large-scale systems, K: Reports National Academy of Sciences, 2009, № 10, 27-35 p.
[8]. One-way functions. / http://crypto.pp.ua /2010/ 06/ odnonapravlennyefunkcii/
[9]. R. Lidl. Finite Fields. Monograph in 2 volumes, T. 1., M.: Mir, 1988. - 432 p.

ПРОТОКОЛ ФОРМУВАННЯ СЕКРЕТНИХ КЛЮЧІВ ШИФРУВАННЯ АБОНЕНТАМИ ВІДКРИТИХ КАНАЛІВ ЗВ'ЯЗКУ НА ОСНОВІ УЗАГАЛЬНЕНИХ МАТРИЦЬ ГАЛУА

У статті розглянуто методи формування секретних ключів шифрування двома абонентами відкритих комунікаційних мереж. У генерації ключа беруть участі обидва абоненти мережі. В основу протоколу обміну ключами покладені алгоритми асиметричної (двоключової) криптографії. Рішення проблеми синтезу ключів припускає обчислення односпрямованих функцій і базується на використанні узагальнених подібних матриць Галуа. В якості матриць перетворення подібності обрані перестановочні матриці. Для матриць Галуа розроблений простий спосіб їх побудови, названий методом діагонального заповнення. Узагальнені матриці Галуа зв'язані відношенням ізоморфізму з елементами, що їх утворюють, і залежать від обраних незвідних поліномів, які породжують матриці. Обговорюються варіанти побудови способів оперативної зміни ключів шифрування в кожному сеансі зв'язку наземних пунктів управління з безпілотними літальними апаратами.

Ключові слова: протокол обміну ключами, узагальнені матриці Галуа, подібні матриці, розширені поля Галуа, відношення ізоморфізму.

ENCAPSULATING SECRET ENCRYPTION KEY SUBSCRIBERS OPEN COMMUNICATION CHANNELS BASED ON GENERALIZED GALOIS MATRIX

The article describes the methods of formation of secret encryption keys two subscribers of public communications networks. The key generation participate both parties network. Based key exchange protocol laid asymmetric algorithms (two-key) cryptography. The solution involves the synthesis of the key functions of the calculation of one-way and is based on the use of such generalized matrix Galois. As the similarity transformation matrix selected permutation matrix. For matrices Galois developed a simple method for constructing them, named by diagonal fill. Generalized matrix Galois related by the isomorphism with the generators and their components depend on the selected irreducible polynomial generating matrix. Discussed options for building the operational methods change the encryption keys for each communication session with the ground control UAV.

Index terms: key exchange protocol, one-way functions, generalized matrix Galois like matrix, extended Galois field, the ratio of isomorphism.

Белецкий Анатолий Яковлевич, доктор технических наук, профессор, заслуженный деятель науки и техники Украины, лауреат Государственной премии Украины в области науки и техники, профессор кафедры электроники Национального авиационного университета.
E-mail: abelnau@ukr.net.
Білецький Анатолій Якович, доктор технічних наук, професор, заслужений діяч науки і техніки України, лауреат Державної премії України в галузі науки і техніки, професор кафедри електроніки Національного авіаційного університету.
Beletsky Anatoly, Doctor of Science, Professor, Honored Scientist of Ukraine, Laureate of the State Prize of Ukraine in Science and Technology, Professor of Department Electronics of National Aviation University.