5429); $111^{64} \equiv 4454^2 \equiv 550(\text{mod}5429)$; $111^{79} \equiv 550 \cdot 1221 \cdot 1343 \cdot 1463 \cdot 190 \equiv 3606(\text{mod } 5429)$

Это значит, что часть сообщения c_1 зашифрована в виде $\omega_1 = 3606$.

Блок c_2 шифруется аналогично: $\omega_2 = 234$.

Передаваемое сообщение состоит из зашифрованной части исходного сообщения ω_1 и ω_2 и открытого ключа, которым являются числа e и n (3606, 79, 5429) и (234, 79, 5429) соответственно. Для расшифровки сообщения адресат должен знать секретный ключ – такое натуральное число $d < n$, для которого выполняется условие $e \cdot d \equiv 1 \ (\text{mod } (\phi(n)))$. Отсюда следует, что взломать сообщение, зашифрованное в системе RSA, можно только найдя d – решение сравнения $ed \equiv 1(\text{mod } \phi(n))$. Исходя из свойств $\phi(n)$: необходимо разложить n на множители, что является очень сложной задачей и гарантом криптографической стойкости RSA.

УДК 512.624.95:378.147.091.3

КРИПТОГРАФИЧЕСКАЯ СИСТЕМА ЭЛЬ ГАМАЛЯ

Студент гр. 10401115 Иванов А.И.
Ассистент Крупенкова Т. Г.
Белорусский национальный технический университет

В настоящее время криптосистемы с открытым ключом считаются наиболее перспективными. К ним относится схема Эль Гамаля, основные положения которой рассматриваются в данной работе.

Криптосистема Эль Гамаля создана американским специалистом по криптографии в 1985 году после появления криптосистемы *RSA*. Она послужила основой для целого ряда систем как шифрования, так и цифровой подписи, использующихся в наше время. В алгоритме Эль-Гамаля существуют некоторые открытые параметры, которые могут быть использованы большим числом пользователей. Они называются параметрами домена. К ним относятся: большое простое число $p \approx 2^q$, где $512 \leq q \leq 102$, то есть имеющее 150–300 десятичных знаков; целое число $\boldsymbol{g}$ — образующая циклической группы Z/pZ *; число $\boldsymbol{y}$, которое вычисляется по формуле $y = g^{X (\text{mod } p)}$. К закрытым ключам относятся: целое число **x** такое, что $1 < x < p$ и сессионный ключ — целое число $\boldsymbol{k}$ такое, что $1 < k < p - 1$

Два секретных ключа $\boldsymbol{x}$ и $\boldsymbol{k}$ являются элементами группы Z /pZ *. Числа ***(p, g, y)*** - тройка открытых ключей криптосистемы Эль Гамаля, число $\boldsymbol{x}$— закрытый ключ.

Передаваемая информация в криптосистеме Эль Гамаля предварительно преобразуется в десятичное число. Сообщение ***c*** должно быть меньше числа **p.** Оно шифруется умножением ***c*** на $K = y^{k \pmod p}$. Число ***c***, рассматривается как элемент группы Z/pZ *.

Зашифрованное сообщение имеет вид $w = c \cdot K \pmod p = c \cdot y^{k \pmod p}$**.** Адресат получает расширенное сообщение $(O_{ck}; w)$**,** где $O_{ck} = g^{k \pmod p}$ - число-подсказка, называемое открытым сеансовым ключом. Получатель послания, зная секретный ключ **x**, возводит O_{ck} в степень **x** и находит число **К** по формуле $O^{x}_{ck} = g^{kx \pmod p} = y^{k \pmod p} = K$. Затем сообщение восстанавливается окончательно с помощью формулы: $w \cdot K^{-1} \pmod p = c$.

Таким образом, криптостойкость рассмотренной системы основана на вычислительной сложности проблемы дискретного логарифмирования. Из-за высокой сложности поиска решения она получила широкое распространение в области защиты данных.

УДК 615.847+616.895.4

ФИЗИОТЕРАПЕВТИЧЕСКИЕ МЕТОДЫ ДИАГНОСТИКИ ДЕПРЕССИВНЫХ СОСТОЯНИЙ ЧЕЛОВЕКА

Студент гр.ПБ-52м (магистрант) Цокота М.В.[1]
Канд. техн. наук, доцент Терещенко Н.Ф.[1],
профессор Тымчик Г.С.[1],
канд. техн. наук Чухраев Н.В.[2]
[1]Национальный технический университет Украины «Киевский политехнический институт»
[2]«Научно-методический центр «Мединтех»

Чувство тревоги это нормальная реакция человека на стрессовую ситуацию. Однако ощущение сильной тревоги большую часть времени в течение длительного периода превращается в медицинскую проблему.

В настоящее время в терапии тревожных расстройств используется комплексный подход, который включает в себя лекарственный электрофорез, электросон, диадинамотерапию и другие. Они основаны на принципе пропускания в тело лекарственных веществ под действием электрического тока, которые приводят к снижению чувствительности периферийных, в том числе болевых, рецепторов, к повышению порога болевого восприятия и т.д. Однако величина влияния является нормированной и не зависит от индивидуальных особенностей.

Однако депрессию можно увидеть, если сделать сканограмму мозга, то есть позитронно-эмиссионную томограмму или КТ-сканирование. Хотя данное сканирования даст врачам возможность выявить заболевания или травмы головного мозга, однако его можно проводить только в