рафії. Вінниця: ВДТУ, 2003. 143 с.
3. Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая стеганография. — М.: "Солон-Пресс", 2002. — 272 с.
4. Вентцель Е.С., Овчаров В.А. Теория вероятностей и её инженерные приложения. Уч. пос. для ВУЗов. — М.: "Академия", 2003. — 464 с.
5. Скляр Б., Цифровая связь: Теоретические основы и практическое применение. М.: "Вильямс", 2003. — 1104 с.

Навроцкий Д.О., Дюжаев Л.,Пузиренко О.Ю **Представление и прогнозирование эффективности нового протокола оценки качества реализации разрабатываемых алгоритмов компьютерной стеганографии** Представлен протокол оценки качества реализации известных и прогнозирование эффективности разрабатываемых алгоритмов компьютерной стеганографии. Предложенную концепцию можно использовать для мониторинга стеганоалгоритмов.	Navrotskiy D.O.,Dyuzhayev L.,Puzirenko O.Yu **Representation and forecasting of efficiency of the new protocol of an estimation of quality of realization of developed algorithms computer steganography** There is represented the protocol quality rating of realization and technologic forecasting of efficiency of well-known and developed algorithms of computer stenography. The proposed concept can be used for the monitoring of steganoalgorithms, which are used for copyright protection.

УДК 621.391

НАДІЙНІСТЬ ЗАХИСТУ ІНФОРМАЦІЇ СИСТЕМИ ЕЛЕКТРОННОГО ЦИФРОВОГО ПІДПИСУ

Танцюра Д.В, Зіньковський Ю.Ф.

Розглянута побудова електронного цифрового підпису, надійність як складових, так і всієї системи вцілому. Приведені рекомендації щодо підвищення надійності системи електронного цифрового підпису.

Для зменшення несанкціонованого доступу, підробок і хакерських атак в мережі Інтернет - необхідні технології аутентифікації суб'єктів мережі(користувачів, серверів, програм). Однією з таких технологій і є електронний цифровий підпис (ЕЦП), який узаконений в Україні з 2003 року.

Використання ЕЦП дозволяє однозначно ідентифікувати автора-відправника(повідомлення); уникнути перехвату, модифікації і підробки повідомлень та інших даних, які пересилаються в мережі. ЕЦП – представляє собою „вживлення" даних фрагменту додаткової зашифрованої інформації, яка слугує для ідентифікації та достовірності повідомлення. Тобто сама інформація, яка підписується – не шифрується(хоча можливе і шифрування). Ця додаткова інформація(ЕЦП) формується двома діями: визначення хеш-функції та шифрування результатів з відкритим ключем. Хеш-функція – це функція перетворення вихідного повідомлення(інформації) певним чином в відповідний повідомленню код – згортку, яка слугує для контролю цілісності даних. Згортка шифрується з відкритим ключем і результат - стає невід'ємною частиною повідомлення(тобто прикріплюється до нього). Шифрування з відкритим ключем особливе тому, що для шифрування і дешифрування використовуються два різні, не випливаючи один з одного, ключі – закритий і відкритий відповідно. Закритий ключ – це той

ключ (набір символів), за допомогою якого відбувається шифрування згортки, і який відомий лише власнику відповідного ЕЦП. Відкритий ключ – це той ключ, який слугує для дешифрування згортки (перевірки ЕЦП), і який публікується центром сертифікації ключів (тобто є загальновідомим).

Система ЕЦП є зручна і корисна, але потребує високої надійності [2], для уникнення(унеможливлення) помилок, і підтвердження юридичної сили пересилаємих документів. Надійність системи ЕЦП залежить від багатьох факторів, основні з яких можна звести до двох наступних: точна ідентифікація(беззбройне, безпомилкове прочитання ідентифікаційної інформації) та уникнення можливості підробки повідомлення чи пересилаємих документів. Перший фактор особливий тим, що важко взяти на себе відповідальність за надійність і безпеку програмної(та апаратної) системи, яка забезпечує ЕЦП. Тому необхідно забезпечити захищеність програмного середовища як використанням програмного захисту та адміністратора безпеки, так і організаційними обмеженнями(правилами та нормами). Особливість другого фактора в тому, що він включає в себе цілу низьку чинників(параметрів), найважливіші з яких: надійність хеш-функції, надійність згортки, надійність алгоритму шифрування з відкритим ключем, надійність закритого ключа, яка визначається насамперед надійністю генератора ключа(його особливостями).

Криптографічна однобічна хеш-функція – функція перетворення інформації(повідомлення), значення якої(згортка) залежить від символів вихідного повідомлення та їх взаємного розміщення(порядку їх слідування); вона має певну фіксовану бітову довжину, яка не залежить від величини повідомлення, і якій притаманні наступні властивості:

1) не існує відомого поліноміального алгоритму обчислень значень оберненої функції(тобто за реальний час неможливо повністю точно відновити вихідну інформацію(повідомлення));
2) не існує відомого ефективного поліноміального алгоритму такого альтернативного вихідного повідомлення, при якому б згортка залишилася незмінною, тобто ідентичною для попереднього повідомлення(не існує колізій).

Найпоширеніші хеш-функції – на основі однокрокових стискувальних функцій [1] двох змінних $y=f(x_1, x_2)$, де x_1, x_2, - двійкові вектори довжини m; y - двійковий вектор довжини згортки n. Для обчислення згортки $h(M)$ повідомлення M розбивають на N блоків $M_1, M_2, ..., M_N$, довжини m. Якщо довжина повідомлення не кратна m, то останній блок спеціальним чином доповнюють до довжини m. До блоків $M_1, M_2, ..., M_N$ застосовують послідовну процедуру обчислення згортки: $H_0=\nu$; $H_i=f(M_i,H_{i-1})$, $i=1,\ldots,N$; $h(M)=H_N$, де ν - деякий фіксований початковий вектор. Якщо функція f залежить від ключа, то за вектор ν можна взяти нульовий, інакше - утворити вектор ν з фрагментів дати, часу, номера повідомлення тощо. Властивості

такої хеш-функції h визначаються властивостями однокрокової стискувальної функції f. Для формування ЕЦП використовують безключові хеш-функції[1]. Основні вимоги до цих функцій – їх однобічність, стійкість щодо колізій та пошуку іншого прообразу. Це означає складність задач щодо пошуку повідомлення з даним значенням згортки, пари повідомлень з однаковою згорткою, іншого повідомлення з тією ж згорткою для даного повідомлення за відомою згорткою. Оскільки функція $g_k(x)=E_k(x)\oplus x$, де E_k – алгоритм блокового шифрування, однобічна за обома аргументами, то на її основі можна побудувати безключову хеш-функцію: $H_0=\nu$; $H_i=f(M_i,H_{i-1})$, $i=1,\ldots,N$; $h(M)=H_N$, визначаючи однокрокову стискувальну функцію однією з формул: $f(x,H) = E_H(x)\oplus x$ або $f(x,H) = E_x(H)\oplus H$.

Сучасні хеш-функції не містять лазівок для хакерів (деякі з них стандартизовані), а надійність значення згортки (стійкість) зростає з її розрядністю. Для захисту значення згортки хеш-функції використовується модель криптосистеми з відкритим ключем, яка народилася у 1976 році, коли У. Діффі і М.Е. Хеллман(США) ввели поняття однобічної (односпрямованої) функції з лазівкою. За їх допомогою шифрування та дешифрування текстів виконується на різних ключах, при цьому знання одного з них не дозволяє практично визначити інший. Це дає змогу зробити один з ключів відкритим без втрати стійкості шифру і тільки законний користувач зберігає інший ключ в таємниці. Визначення значення x за відомим значенням функції $y=F(x)$ – завжди можна виконати поступовим перебором усіх можливих значень даної функції, поки для якого-небудь x обчислене значення $F(x)$ не буде дорівнювати заданому відомому значенню y. Проте при великих розмірах області визначення функції такий спосіб стає практично нездійсненним. Для відновлення відкритого тексту необхідна не просто однобічні функції, а однобічні функції з лазівкою, які є узагальненням однобічних функцій [1].

Функція $y=F(k,x)$, що залежить від параметра k, є однобічною функцією з лазівкою, якщо:

- існує поліноміальний алгоритм обчислення значень функції $F(k,x)$ для всіх аргументів $x \in X$ і всіх значень параметра k;
- не існує поліноміального алгоритму обчислення значень оберненої функції при невідомому параметрі k, тобто визначити значення аргументу x за відомими значенням функції y при невідомому параметрі k – неможливо;
- існує поліноміальний алгоритм обчислення значень оберненої функції при відомому параметрі k, тобто легко знайти значення аргументу x за відомими y і k.

На сьогодні не побудовано жодної функції, яку б можна було вважати за однобічну функцію або однобічну функцію з лазівкою, не доведено навіть їх існування. В реальних задачах використовують декілька функцій,

які б могли виявитися однобічними функціями з лазівкою, але й для них поки не доведено відсутність поліноміального алгоритму інвертування. Тому на практиці друга вимога в означенні однобічних функцій замінюється більш слабкою: при невідомому параметрі *k ймовірно* не існує поліноміального алгоритму обчислення значень оберненої функції. Але поява нових математичних методів та прогрес обчислювальної техніки можуть зумовити появу таких алгоритмів. Тому на даний час використовують потенційні однобічні функції з лазівкою(множення, піднесення степеня у скінченному полі, задачі кодування-декодування лінійних кодів тощо), для яких ще не знайдено поліноміальних алгоритмів обчислення значень обернених функцій

Існує багато прихованих (не оприлюднених) алгоритмів шифрування. Але їх надійність сумнівна, бо в основному вона тримається на самій секретності, або автор алгоритму сам невпевнений в його надійності (як показує досвід). Тому надійними можна вважати ті алгоритми, які загальновідомі і перевірені часом або якісно проаналізовані крипто-аналітиками. Зазвичай використовують різні алгоритми, але вони стандартизовані і пронумеровані, й кожний користувач знає, який алгоритм (відкритий) використовується. Наприклад, алгоритм *RSA*(від перших літер прізвищ її авторів – *R. Rivest*, *A. Shamir*, *L. Adleman*) — міжнародний. Країни ЄС використовують близько 35 різних криптографічних алгоритмів, Україна — 3, але жоден з них не є стандартом ЄС.

Найбільш поширена серед криптосистем з відкритим ключем - система *RSA* [1]. В основі криптосистеми лежить той факт, що розкласти велике складене число на прості множники досить обчислювано обтяжливе. Процедура шифрування за схемою *RSA* полягає в модульному піднесенні до ступеня за допомогою функції $E(x) = x^e (\mathrm{mod}\ n)$ а процедура дешифрування - у розв'язанні порівняння $D(x) = x^d (\mathrm{mod}\ n)$, де e – частина значення ключа шифрування, d - частина значення ключа дешифрування. Розглянемо цю процедуру шифрування в загальному випадку. Виберемо число $n = pq$ - ціле число, що дорівнює добутку двох великих простих чисел p та q. Виберемо числа e і d з умовою $e \cdot d \equiv 1 (\mathrm{mod}\ \varphi(n))$, де $\varphi(n) = \varphi(p) \cdot \varphi(q) = (q-1) \cdot (p-1)$ - значення функції Ейлера. За відкритий ключ k_2, візьмемо числа n і d, а за закритий ключ k_1-числа p, q, e. Нехай M-відкритий текст, C-криптограма. Тоді рівняння шифрування та дешифрування у системі *RSA*(для ЕЦП) відповідно визначаються формулами $C = E_{k1}(M) \equiv M^e (\mathrm{mod} n)$; $M = D_{k2}(C) \equiv C^d (\mathrm{mod} n)$.

Аналізуючи процедуру шифрування за схемою *RSA* можна зробити висновок, що супротивник може зламати шифр, тільки знаючи закритий ключ e, значення якого можна дізнатися у двох випадках: якщо відоме розкладання числа n на прості множники, або відомий модуль $\varphi(n)$ у порівнянні з $e \cdot d \equiv 1 (\mathrm{mod}\ \varphi(n))$. Оскільки $n = pq$, $\varphi(n) = (p-1)(q-1) = pq - (p+q) + 1$ *і* $(p-q)^2 = p^2 + q^2 - 2pq = (p+q)^2 - 4pq$, то приходимо до системи рівнянь:

$$\varphi(n)=pq-(p+q)+1;\ (p-q)^2=(p+q)^2-4pq$$

Звідси випливає, що, з одного боку, розв'язати систему відносно p і q можливо тільки при відомому значенні $\varphi(n)$, а з другого - знаючи p і q, легко обчислити $\varphi(n)$. Таким чином, обидва випадки, в яких можна визначити закритий ключ, еквівалентні і становлять задачі однієї складності. Тому для надійності алгоритму пропонується вибирати такі значення простих чисел p та q, для яких значення n – буде досить великим для стійкості до загрози з можливими параметрами продуктивності злому.

Секретні ключі є основою криптографічних перетворень - стійкість шифрувальної системи визначається лише таємністю ключа. Основна проблема класичної криптографії довгий час полягала в труднощі генерування непередбачених двійкових послідовностей великої довжини із застосуванням короткого випадкового ключа. Для її рішення широко використовуються генератори двійкових псевдовипадкових послідовностей.

Побудова ідеальних стохастичних пристроїв викликає певні труднощі, тому на практиці легше використовувати псевдовипадкові послідовності чисел, які можна побудувати за допомогою арифметичних алгоритмів (генераторів). Найбільш поширені випадкові числа, що рівномірно розподілені на відрізку [0;1], та рівноймовірні двійкові випадкові знаки α_n з умови $P\{\alpha_n = 0\} = P\{\alpha_n = 1\} = 1/2$ (тоді випадковою послідовністю бітів довжини n буде випадкова величина, яка набуває кожне значення із $\{0;1\}^n$ з однаковою ймовірністю $(1/2)^n$).

До псевдовипадкових послідовностей чисел висунемо вимоги:

- неможливе визначення члена α_{n-1} числової послідовності на основі її відомого наступного фрагмента α_n , α_{n+1}, α_{n+2},..., α_{n+p-1} скінченної довжини p (непередбачуваність генератора ліворуч);
- неможливе визначення члена α_{n+1} числової послідовності на основі її відомого попереднього фрагмента α_{n-p+1} , ..., α_{n-2}, α_{n-1} , α_n скінченної довжини p (непередбачуваність генератора праворуч);
- приблизно однакові ймовірності появи числових знаків у послідовності;
- псевдовипадкова послідовність повинна, мати великий період;

Для високої надійності пропонується використовувати криптостійкі генератори, наприклад–„непередбачувані ліворуч генератори псевдовипадкових числових послідовностей”. Тоді криптоаналітик, навіть знайомий з принципом роботи генератора, але не знайомий з ключами, аналізуючи фрагмент вихідної послідовності α_n , α_{n+1}, α_{n+2},..., α_{n+p-1} може визначити попередній член (α_{n-1}) тільки за допомогою випадковості (наприклад жереба). При такому підході достатньо створити генератор керуючись першою вимогою до псевдовипадкової послідовності, але для більш високої надійності - пропонується щоб генератор задовольняв одночасно всім чотирьом умовам.

Доцільно запропонувати статистично безпечний генератор, який повинен задовольняти наступним вимогам:

- жоден статистичний тест(наприклад за коефіцієнтом безлічної кореляції R) не повинен відрізняти вихідну псевдовипадкову числову послідовність від істинно випадкової;
- усі вихідні числові псевдовипадкові послідовності – рівноймовірні $P(\alpha_0) = P(\alpha_1) =\ldots= P(\alpha_n)$, незалежно від інформації, що подається на вхід генератора;
- усі вихідні числові послідовності мають бути статистично незалежними псевдовипадковими послідовностями.

Однобічна функція з лазівкою дає змогу побудувати криптографічні стійкі генератори псевдовипадкових – двійкових послідовностей. Такі генератори базуються на тих же важкорозв'язувальних задачах, що й криптографія з відкритим ключем - факторизація складеного числа, добування коренів за модулем, дискретне логарифмування. Наприклад, генератор *BBS* (генератор квадратичних лишків) - простий та ефективний генератор, що використовує складність факторизації великих чисел. Принцип побудови генератора – пропонується наступним:

1. Навмання вибираються прості числа p і q (великі прості числа, приблизно однакового розміру) з властивістю $p\equiv 3(\text{mod } 4)$, $q\equiv 3(\text{mod } 4)$ та обчислюється ціле число Блюма ($p\equiv q\equiv 3(\text{mod } 4)$) $n = pq$, ці числа p і q зберігаються у таємниці.

2. Випадково вибирається з мультиплікативної групи лишків Z_n^* інше ціле число x, взаємно просте з числом n.

3. Обчислюється число $x_0\equiv x^2(\text{mod } n)$, яке буде початковим значенням генератора.

4. За законом $x_i\equiv x^2_{i-1}(\text{mod } n)$ утворюється послідовність чисел x_i.

5. Шукана псевдовипадкова двійкова послідовність $b_1b_2\ldots b_m$ ($BBS_{n,m}(x_0)$) - послідовність молодших бітів чисел x_i, тобто $b_i= x_{i-1}(\text{mod } 2)$, $i=\overline{1;m}$.

Одна з найцікавіших властивостей генератора – можливість визначати i-й біт псевдовипадкової послідовності без завчасного обчислення i-1 попередніх бітів за умови, що відоме розкладання модуля n на множники. Дійсно, за теоремою Ейлера $x^{\varphi(n)}\equiv 1(\text{mod } n) => x^{(p-1)(q-1)}\equiv 1(\text{mod } n)$, а відтак $x_i\equiv x_0^{2i\ (\text{mod}(p-1)(q-1))}(\text{mod } n)$. Звідси випливає, що завдяки двом модульним піднесенням до степеня, які ефективно обчислюються, будь-яке число x_i, визначається тільки з початкового значення x_0 та свого індексу.

Здатність генератора *BBS* протистояти зламу базується на складності розкладання числа n на множники. Визначити член x_{i-1} послідовності можна наступним чином:

- за бієктивністю функції $f(x)= x^2(\text{mod } n)$, на множині Q_n квадратичних лишків за модулем n елемент x_{i-1} однозначно визначається умовами: $x_i\equiv x^2_{i-1}(\text{mod } n)$, $x_i \in Q_n$;

- за наслідком теореми про лишки $a = x_{i-1} \bmod p$; $b = x_{i-1} \bmod q$ задовольняють два порівняння $a^2 = x_i \bmod p$ і $b^2 = x_i \bmod q$. Пара чисел a та b однозначно визначає й саме число x_{i-1}. Добування кореня за модулем p, для якого $p \equiv 3 (\bmod 4)$, еквівалентне піднесенню до степеня $(p+1)/4$. Отже, для знаходження чисел a і b доцільно запропонувати співвідношення $a = x_i^{(p+1)/4} \bmod p$ та $b = x_i^{(q+1)/4} \bmod q$.

Можна зробити висновок, що надійність генератора підвищується разом зі збільшенням множини значень розкладу числа n на множники.

Пропонується побудувати генератор псевдовипадкових двійкових послідовностей за допомогою інших однобічних функцій з лазівкою, наприклад функції, що є основою криптосистеми *RSA*. Початковими параметрами генератора *RSA* є модуль $n = p \cdot q$, де p і q - два великих простих числа (закритий ключ), ціле число e, взаємно просте з числом $(p-1)(q-1)$, та випадкове початкове число $x_0 < n$. Числова послідовність утворюється за законом $x_{i+1} \equiv x_i^e (\bmod n)$. На вихід генератора подається молодший біт числа x_i. Явно видно, що безпека такого генератора спирається на складність зламу криптосистеми *RSA* при великих n (розкладання числа n на множники).

Проведена оцінка генераторів *BBS* та *RSA* дає можливість визначення надійності таких генераторів, яка обмежується тільки величиною числа n, але навіть при його великому значенні існує значна можливість злому таких генераторів. Для зменшення ймовірності злому пропонується створити такий генератор, надійність якого не буде визначатися тільки складністю розкладання на множники великого числа. Тому надійність шифрування залежить і від складності самого ключа, як видно з аналізу роботи її (системи шифрування) складових.

У загальному випадку під надійністю обчислювальної системи розуміють властивість системи виконувати покладені на неї функції протягом заданого проміжку часу. Стосовно системи захисту інформації ЕЦП можна визначити надійність, як властивість системи забезпечувати захист (стійкість до злому) комп'ютерної інформації протягом заданого проміжку часу. Виходячи з складності ключа N (як основного параметра безпеки) визначимо ймовірність злому за певний термін: $S = TG / N$, де S – шанс злому, T – час зламування шифру, G – швидкість підбору ключа, N – складність ключа(кількість можливих варіантів). Тоді ймовірність захисту (стійкості) протягом певного терміну можна записати як $P = 1 - S = 1 - TG/N = (N - TG)/N$. Видно, що зі збільшенням часу зламу ймовірність надійного захисту спадає, а зі збільшенням складності ключа N – зростає.

Доцільно визначити не надійність ключа певної складності, а необхідну складність ключа [3] при заданій (необхідній) надійності, спираючись на технічні можливості джерела загрози: $N = TG / S$, де N–необхідна складність ключа, T–час життя шифру(необхідна), G–швидкість підбору ключа, S–шанс злому (вірогідність знаходження ключа раптово) за певний термін.

Час життя ключа зазвичай приймають менше 25 років. Наприклад, у Британії секретні урядові рішення через 25 років публікують для істориків.

Швидкість підбору ключа викликає великі суперечки через великий розкид параметрів швидкодії апаратних засобів та час створення ЕОМ з необхідною високою швидкодією. Шанс злому досить індивідуальна величина, яку зазвичай приймають $S=10^{-3}\ldots10^{-8}$, в залежності від сфери застосування. При відомій необхідній складності ключа визначаємо розрядність ключа $B=\log_2 N(bit)$. Випадкові числа повинні ґрунтуватися на дійсному фізичному джерелі випадкової інформації, що неможливо пророчити.

Для ускладнення зламу крипто-аналітиками, як потенційними хакерами, генератори гами (псевдовипадкових послідовностей) будуються на комбінації двох або більше генераторів з використанням нелінійних логічних функцій. Але розвиток сучасної техніки дає можливість зламувати комбінацію з двох генераторів (якщо генератор не ґрунтується на фізичному джерелі випадкової інформації). Тому для побудови високонадійних крипто-стійких генераторів створюють комбінації більше ніж двох генераторів з використанням нелінійних логічних функцій, або на фізичному джерелі випадкової інформації, та їх поєднанні.

Висновки

Надійність (стійкість) системи ЕЦП залежить від багатьох факторів, у тому числі і від її структури. Для підвищення надійності системи вцілому необхідно підвищувати, в першу чергу, надійність найслабкіших ланок - ключів шифрування і генераторів випадкових послідовностей, за рахунок відповідно підвищення складності та створення комбінацій. Розвиток сучасної криптографії дає можливість вирішувати проблеми надійності криптографічних засобів захисту інформації, ліквідувати їх слабкі місця та створювати ефективні високонадійні хеш-функції, алгоритми шифрування та генератори псевдовипадкових послідовностей, потреба в яких не зменшується.

Література

1. Математичні основи криптографії: Навч. посібник / Г.В. Кузнєцов, В.В., та ін. – Дніпропетровськ: Національний гірничий університет, 2004. – Ч. 1. – 391 с.
2. Ивт И., Богданов В. „Надежна ли цифровая подпись?” // www.sdteam.com
3. Ильчук Е.В. "Введение в криптографию" // www.nerungri.edu.ru

Танцюра Д.В., Зиньковский Ю.Ф.

Надёжность защиты информации системы электронной цифровой подписи

Рассмотрено построение електронной цифровой підписи, надёжность как составных частей, так и системы в целом. Приведены рекомендации по повышению надёжности системи.

Tantsyura D. V., Zinkovskiy Y. F.

Reliability of protection of the information of a system of an electronic digital signature

The construction of an electronic digital signature, reliability both compound, and system is reviewed. The guidelines concerning a reliability augmentation of a system of an electronic digital signature are adduced.