СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Орлов А. ArchiCAD. Начали! : учебный курс / А. Орлов. — СПб. : Питер, 2008. — 160 с.
2. Столяровский С. ArchiCAD 11: учебный курс / С. Столяровский. — СПб.: Питер, 2008. — 336 с.
3. Ланцов А. Л. Компьютерное проектирование в архитектуре ARCHICAD 11 / А.Л. Ланцов. – М. : ДМК Пресс, 2007. – 800 с.
4. Зеленина В.Г. САПР в строительстве. Архитектура : учебное пособие / В.Г. Зеленина, С.Г. Пуйсанс. – Пермь : Изд-во Перм. гос. техн. ун-та, 2007. — 232 с.
5. Титов С. ArchiCAD 10 : Справочник с примерами / С.Титов. — М. : КУДИЦ-ПРЕСС, 2007. — 560 с.
6. ArchiCAD [Електронний ресурс]. – Режим доступу : http://uk.wikipedia.org/wiki/ArchiCAD . – Назва з екрана.
7. Леонтьев Б.К. Как построить дом с помощью персонального комп'ютера / Б.К. Леонтьев — М : НТ Пресс, 2006. — 223 с.

Зозуля М.

Науковий керівник – доц. Горбатюк Р.М.

АНАЛІЗ РОБОТИ КРИПТОСИСТЕМИ RC6

Проблема захисту інформації являє собою сукупність тісно зв'язаних підпроблем в області права, організації керування, розробки технічних засобів, програмування і математики. Ефективну систему захисту можна створити шляхом об'єднання зусиль різних фахівців. Одна з центральних задач проектування систем захисту полягає у раціональному розподілі людських, матеріальних та інших ресурсів.

Відомо, що шифрування й дешифрування даних відбувається за допомогою симетричних та асиметричних криптосистем, причому до появи останніх єдиними існуючими були симетричні криптосистеми.

Симетричні криптосистеми – це спосіб шифрування, в якому один і той самий криптографічний ключ, що обирається перед обміном інформації та зберігається в секреті, застосовується як для шифрування, так і для дешифрування, при цьому інформація може шифруватися потоком або блоками [1].

На сьогодні все більшої ваги набуває проблема захисту інформації від несанкціонованого доступу при передачі й зберіганні інформації. Сутність цієї проблеми - постійна боротьба фахівців із захисту інформації зі своїми "опонентами" – криптоаналітиками. Одним із методів такої боротьби є створення алгоритмів шифрування інформації. Існує велика кількість алгоритмів шифрування, проте одним із найбільш успішних та криптостійких є алгоритм RC6.

Шифр RC6 відповідає вимогам Advanced Encryption Standard (Розширеному Стандарту Шифрування) (AES). Подібно до шифру RC5, RC6 розробили з істотним використанням залежних від даних раундів шифрування. Нові особливості RC6 включають використання чотирьох працюючих регістрів замість двох, і включення цілого числа, як додаткову примітивну операцію.

RC6 – це новий блоковий шифр, який був представлений на розгляд NIST (Національний інститут стандартів та технології). Проект шифру RC6 почався з розгляду RC5, як потенційного кандидата для AES. Але зміни, які були потім зроблені, суттєво збільшили захист шифру та покращили його роботу. Схема роботи алгоритму шифрування RC6 зображена на рис. 1.

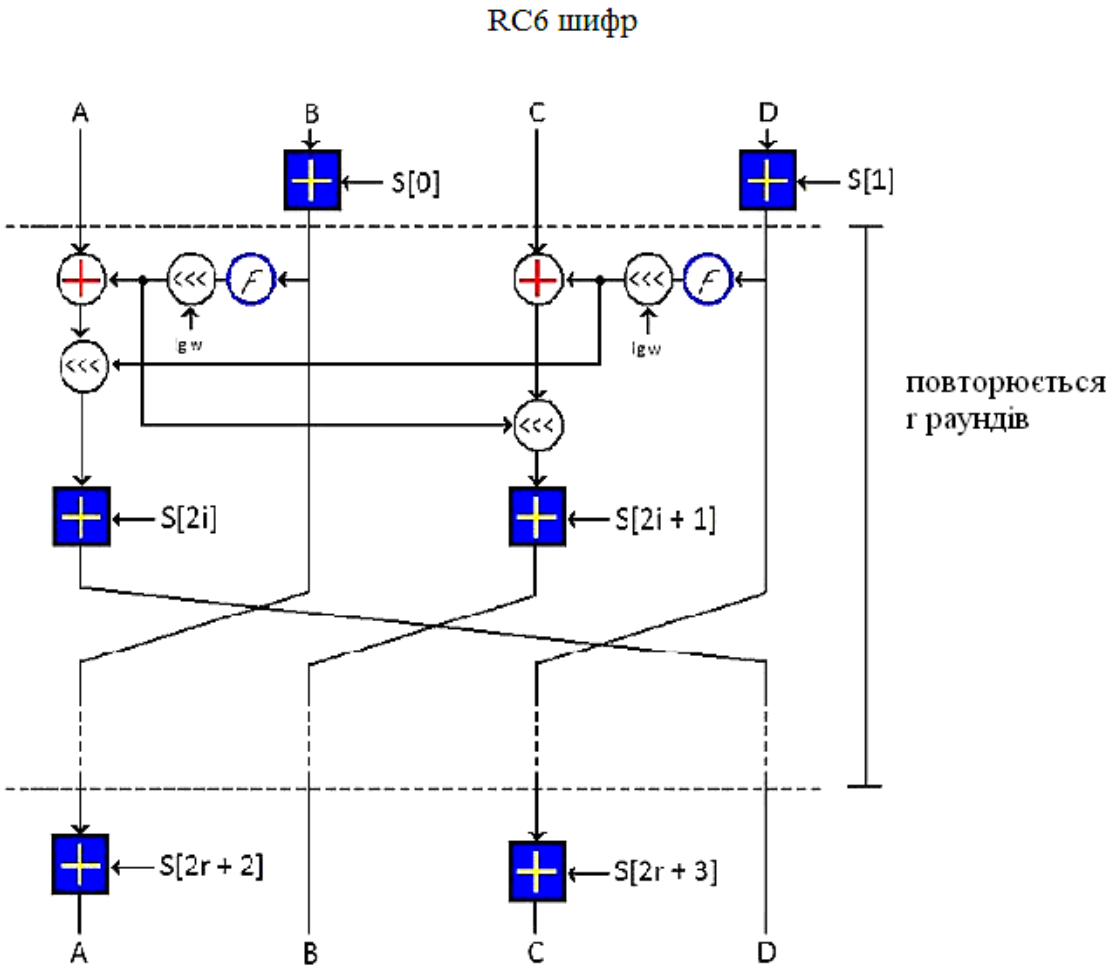


Рис. 1. Схема роботи алгоритму шифрування RC6

Шифр RC6 підтримує блоки довжиною 128 біт і ключі довжиною 128, 192 і 256 біт, але сам алгоритм, як і RC5, може бути налаштований для підтримки більш широкого діапазону довжин, як блоків, так і ключів (від 0 до 2040 біт) [2]. RC6 подібний до RC5 за своєю структурою і є простим у реалізації. Однак одна з примітивних операцій – операція множення, повільно виконується на низько продуктивному обладнанні та ускладнює реалізацію шифру на ряді апаратних платформ. У даному випадку алгоритм шифрування втрачає одну зі своїх ключових переваг - високу швидкість виконання, що стало причиною для критики і однією з перепон для обрання в якості нового стандарту. Однак, на системах з процесором Pentium II, Pentium Pro, Pentium III, PowerPC і ARM алгоритм RC6 випереджає Rijndael (симетричний алгоритм блочного шифрування).

Так само, як і RC5, RC6 – параметризована сім'я алгоритмів шифрування. Для специфікації алгоритму з конкретними параметрами, прийнято позначення RC6-w/r/b, де :

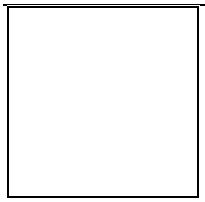
w – довжина машинного слова в бітах;

r – число раундів;

b – довжина ключа в байтах.

Варіант алгоритму RC6 підтримує блоки довжиною 128 біт і ключі довжиною 128, 192 і 256 біт, а також містить 20 раундів. Тобто RC6-128/20/b, де b = 128,192 або 256 біт. У відношенні такого алгоритму ніяких атак не було виявлено. Проте були виявлені атаки проти спрощених версій алгоритму, тобто алгоритму зі зменшеною кількістю раундів.

Вважається, що кращий варіант нападу на RC6 доступний для криптоаналітика, є повним перебором b-байтового ключа шифрування (або розширений ключовий масив S [0, ..., 43], коли наданий користувачем ключ шифрування особливо довгий). Для повного перебору потрібно



операцій. Дон Копперсміт [3] зауважив, що за рахунок значної пам'яті і попереднього обчислення можна організувати атаку «meet-in-the-middle», щоб відновити розширений ключовий масив S [0, ..., 43]. Більш просунуті атаки, такі як диференційний і лінійний криптоаналіз, здійснимі на версіях шифру з незначною кількістю раундів, складно здійснимі для нападу на повний шифр RC6 з 20 раундами. Складність полягає в тому, що важко знайти хороші повторювані особливості або лінійні наближення, з якими могла б бути здійснена атака.

З огляду на сказане, можна підсумувати вимоги з безпеки RC6 наступним чином:

- кращою атакою на RC6 є повний перебір для забезпеченого користувачем ключа шифрування;

- вимоги до даних, щоб організувати більш складні атаки на RC6, такі як диференційний і лінійний криптоаналіз, перевищують доступні дані.

Важливим критерієм резерву безпеки є максимальне число раундів, при якому можлива атака. Це можливо для 12 -, 14 - і 15 - раундових варіантів RC6.

Для більшості додатків впровадження RC6 у програмне забезпечення – ймовірно, кращий вибір. Примітивні операції RC6 (додавання, віднімання, множення, виключення або зсув) підтримуються сучасними мікропроцесорами і тому під час їх розробки це враховували. Однак, у деяких випадках корисно мати RC6 у вигляді вбудовуваної схеми. Тоді можна було б досягти максимальної швидкості або об'єднати інші функції навколо RC6. Оскільки RC6 використовує примітивні операції, описані вище, то можна використовувати переваги існуючої перевірки в процесі розробки схемних модулів для реалізації цих примітивних операцій. Наприклад, якщо реалізувати RC6 використовуючи технології, засновані на матрицях логічних елементів, то це не принесе бажаних переваг навіть через значні зусилля, які треба буде докласти для розробки схеми множень. Реалізація алгоритму на базі такої технології значно поступається реалізації на базі процесора. Але це нетипова ситуація і можна легко спроектувати схему множення, яка буде використовуватися в якості підмодуля [3]. З 20 раундами на блок час шифрування приблизно дорівнює 100 наносекунд для кожного блоку, забезпечуючи передбачувану швидкість передачі даних приблизно 1.3 Гбіт / сек.

Як випливає з опису алгоритму, RC6 – компактна криптосистема. Дійсно, реалізація алгоритму RC6 на Асемблері для мікропроцесора Intel Pentium Pro може бути здійснена на 256 байтах коду і менше для кожної задачі та установки ключа блоку шифрування блоку дешифрування. На відміну від багатьох інших алгоритмів шифрування RC6 не використовує довідкові таблиці під час шифрування. Це означає, що код RC6 і дані можуть міститися в сучасній кеш-пам'яті, і тим самим економити місце в пам'яті. Враховуючи, що RC6 повністю параметризується, шифр є універсальним.

RC6 схожий на RC5 – розрахунок підключа проводиться тим же способом. Програмні реалізації RC6 є найшвидшими серед алгоритмів шифрування, під час забезпечення достатньої стійкості шифру. Представлений нижче модуль побудований за тим же принципом, що і попередні - імена функцій збігаються, і якщо є потреба замінити в програмі шифрування з IDEA або RC5 на RC6 - потрібно просто додати модуль RC6, а IDEA або RC5 - видалити зі списку uses. Шифр RC6, на відміну від RC5, оперує блоками по 16 байт, а модуль побудований так, що під час шифрації методами: EncryptCopy, DecryptCopy, EncryptStream, DecryptStream розмір даних не буде кратний 16 - останній блок довжиною 1 .. 15 байт не шифрується і в "чистому" вигляді додається до зашифрованих. Також і при дешифруванні - якщо останній блок розміром 1 .. 15 байт він не дешифрується, а додається до розшифрованих даних. Такий підхід забезпечує "симетричне" шифрування, оскільки розміри вхідних і вихідних даних повністю збігаються. Однак такий підхід призводить до деяких складнощів – останній блок потребує шифрування. На наш погляд кращий вихід із цієї ситуації - додати під час шифрування до вихідних даних рядок певної довжини і після дешифрування відкинути з кінця рядок тієї ж довжини [4].

RC6 надає користувачеві гнучкість щодо розміру ключа шифрування, числа раундів і розміру слова основного обчислювального модуля. У той час як RC6, представлений для розгляду на AES, базується на використанні 32-розрядних слів (розмір блоку 128 біт), потреби ринку потребують розширення RC6 для інших розмірів блоку. Найбільшу цікавість представляють розміри блоку в 256 біт, які використовували б розмір слова 64 біт і продуктивність, пропоновану наступним поколінням системної архітектури. Зазначимо, що структура RC6 дозволяє експлуатувати певну ступінь аналогії в підпрограмах розшифровки і шифрування. Наприклад, обчислення t і u в кожному раунді можна бути вирахувати паралельно, як і поновлення A і C. Оскільки процесори розвиваються в напрямі збільшення кількості внутрішнього паралелізму (наприклад, з переміщенням до суперскалярної архітектури), реалізації RC6 повинні продемонструвати велику продуктивність.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Merkle R. Secure Communications over Insecure Channels (1974): A history of the idea and its publication [Електронний ресурс] – Режим доступу :
2. http://www.itas.fzk.de/mahp/weber/merkle.htm. – Secure Communikations over Insecure Chanels.
3. Rivest R.L. The RC6 Block Cipher. v1.1 / R.L.Rivest, M.J.B. Robshaw, R.Sidney, Y.L. Yin [Електронний ресурс] – Режим доступу : http://www.rsa.com/rsalabs/aes/ (20.08.1998). – The RC6 Block Cipher..
4. J.-L. Beuchat. Etude et conception d'op´erateurs arithm´etiques optimis´es pour circuits programmables. PhD thesis, Swiss Federal Institute of Technology Lausanne, 2001. – 320 p.
5. Модуль для RC6 шифрування [Електронний ресурс]. – Режим доступу: http://www.delphisources.ru /pages/faq/base/rc6_encryption.html.

Диндура Р.

Науковий керівник – проф. Терещук Г.В.

РОЗВИТОК ХУДОЖНЬОЇ ТВОРЧОСТІ МАЙБУТНІХ УЧИТЕЛІВ ТЕХНОЛОГІЙ НА ГУРТКОВИХ ЗАНЯТТЯХ ІЗ ДЕКОРАТИВНО-ПРИКЛАДНОГО МИСТЕЦТВА

В епоху стрімкого розвитку науки і техніки, впровадження інтенсивних технологій і пов'язаних з ними технічних засобів підготування майбутніх вчителів технологій має бути орієнтованя на формування особистісних якостей, соціально-значимих знань, ціннісних орієнтацій, збереження та примноження культурної спадщини українського народу.

Сучасні умови професійної діяльності вчителя технологій вимагають від нього значного творчого потенціалу, високого рівня інтелектуального розвитку та творчого мислення. Рівень суспільного буття, зростання матеріальних і духовних потреб особистості, необхідність гармонізації стосунків людини і довкілля вимагають розвитку в майбутніх фахівців творчих сил, устремлінь будувати своє життя за законами добра і краси. Тому суспільство формує соціальне замовлення на фахівців, які володіють творчими здібностями і мають бездоганний естетичний смак. Очевидно, що прищеплювати такий смак і розвивати художню творчість майбутнього вчителя трудового навчання треба на гурткових заняттях, головна роль тут відводиться гуртковим заняттям з декоративно-прикладного мистецтва. На жаль, у підготовці вчителів технологій є ще багато неузгоджених питань, а естетично-художньому вихованню та розвитку художньо-творчих умінь і навичок відводиться занадто мало місця [3, с. 1].

Творчість розглядається як найважливіша професійна характеристика та важлива особистісна якість майбутнього вчителя, яка дозволяє легко орієнтуватися в швидко мінливих соціальних умовах та інформаційному полі, яке постійно розширюється.

На особливу роль мистецтва, художньої творчості в естетичному, моральному та трудовому вихованні молоді, формуванні творчої особистості вказують у своїх працях психологи і педагоги-дослідники, серед яких А.А. Аронов, І.А. Зязюн, М.С. Каган, В.І.Мазепа, Л.М. Масол, Н.Г. Ничкало, Л.О. Новак, О.М. Отич, В.О. Радкевич, О.П. Рудницька, О.П. Тищенко та інші.

Проте, в наявних працях не розкрито повністю роль вчителя технологій в розвитку творчого мислення студентів та їхніх художніх здібностей. Процес його підготовки досліджувався багатьма науковцями, серед яких Г.С. Альтшуллер, Р.С.Гуревич, О.М. Коберник, В.М. Мадзігон, В.О. Моляко,