[**Лабораторна робота № 3**](http://vns.lp.edu.ua/mod/page/view.php?id=197093)

**СТВОРЕННЯ ПРОГРАМНОГО ЗАСОБУ ДЛЯ ЗАБЕЗПЕЧЕННЯ КОНФІДЕНЦІЙНОСТІ ІНФОРМАЦІЇ**

**Мета роботи:** ознайомитись з методами криптографічного забезпечення конфіденційності інформації, навчитись створювати комплексні програмні продукти для захисту інформації з використанням алгоритмів симетричного [шифрування](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8932&eid=187834&displayformat=dictionary), хешування та генераторів псевдовипадкових чисел.

**Теоретичні відомості.**

[RC5](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8932&eid=187748&displayformat=dictionary) – це алгоритм симетричного [шифрування](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8932&eid=187834&displayformat=dictionary), розроблений Роном Райвестом в середині 90-х років. При розробці [RC5](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8932&eid=187748&displayformat=dictionary) ставилась задача досягнення наступних характеристик.

        **Придатність для апаратної та програмної реалізації.** В [RC5](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8932&eid=187748&displayformat=dictionary) використовуються тільки елементарні обчислювальні операції, які зазвичай застосовуються в мікропроцесорах.

        **Швидкість виконання.** [RC5](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8932&eid=187748&displayformat=dictionary) є простим алгоритмом, що працює з даними розміром в машинне слово. Усі основні операції передбачають також роботу з даними довжиною в слово.

        **Адаптованість до процесорів з різною довжиною слова.** Довжина слова в бітах є параметром [RC5](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8932&eid=187748&displayformat=dictionary) – при зміні довжини слова змінюється сам алгоритм.

        **Змінна кількість раундів.** Кількість раундів є другим параметром [RC5](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8932&eid=187748&displayformat=dictionary). Цей параметр дозволяє вибрати оптимальне співвідношення необхідної швидкості роботи і вимог до ступеня захисту.

        **Змінна довжина ключа.** Довжина ключа є третім параметром [RC5](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8932&eid=187748&displayformat=dictionary). Як і в попередньому випадку, цей параметр дозволяє знайти прийнятний компроміс між швидкістю роботи та необхідним рівнем безпеки.

        **Простота.** Структура [RC5](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8932&eid=187748&displayformat=dictionary) дуже проста не тільки для реалізації, але й для оцінки її криптоаналітичної стійкості.

        **Низькі вимоги до пам'яті.** Низькі вимоги до пам'яті роблять [RC5](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8932&eid=187748&displayformat=dictionary) придатним для використання в смарт-картах та інших подібних пристроях з обмеженим об'ємом пам'яті.

        **Високий ступінь захисту.** [RC5](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8932&eid=187748&displayformat=dictionary) покликаний забезпечити високий ступінь захисту за умови вибору відповідних значень параметрів.

        **Залежність циклічних зсувів від даних.** В [RC5](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8932&eid=187748&displayformat=dictionary) використовуються циклічні зсуви, величина яких залежить від даних, що повинно підвищувати криптоаналітичну [стійкість](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8932&eid=187822&displayformat=dictionary) алгоритму.

Алгоритм [RC5](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8932&eid=187748&displayformat=dictionary) вбудований в багатьох основних продуктах компанії [RSA](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8932&eid=187747&displayformat=dictionary) Data Security Inc., включаючи BSAFE, JSAFE та S/MAIL.

RC5 фактично являє собою родину алгоритмів [шифрування](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8932&eid=187834&displayformat=dictionary), що визначається трьома наступними параметрами (табл. 3).

Таблиця 3. Параметри алгоритму [RC5](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8932&eid=187748&displayformat=dictionary)

|  |  |  |
| --- | --- | --- |
| **Параметр** | **Визначення** | **Допустимі значення** |
| *w* | Розмір слова в бітах. RC5 шифрує дані блоками довжиною в 2 слова | 16, 32, 64 |
| *r* | Кількість раундів | 0, 1, …, 255 |
| *b* | Кількість 8-бітових байтів (октетів) в таємному ключі *К* | 0, 1, …, 255 |

Таким чином, [RC5](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8932&eid=187748&displayformat=dictionary) шифрує блоки відкритого тексту довжиною 32, 64 чи 128 бітів в блоки шифрованого тексту тієї самої довжини. Довжина ключа може змінюватись від 0 до 2040 бітів. Конкретна версія [RC5](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8932&eid=187748&displayformat=dictionary) позначається [RC5](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8932&eid=187748&displayformat=dictionary)-*w*/*r*/*b*. Наприклад, RC5-32/12/16 використовує 32-бітові слова (64-бітові блоки відкритого і шифрованого тексту), 12 раундів [шифрування](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8932&eid=187834&displayformat=dictionary) і ключ довжиною 16 байтів (128 бітів). Райвест пропонує використовувати [RC5](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8932&eid=187748&displayformat=dictionary)-32/12/16 в якості "стандартної" версії [RC5](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8932&eid=187748&displayformat=dictionary).

В алгоритмі [RC5](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8932&eid=187748&displayformat=dictionary) виконуються три елементарні операції (а також обернені до них):

        **Додавання.** Додавання слів, позначене символом +, виконується по модулю 2*w*. Обернена операція, позначена символом -, є відніманням по модулю 2*w*.

        **Побітове виключне АБО.** Ця операція позначається символом .

        [**Циклічний зсув**](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8932&eid=187827&displayformat=dictionary)**вліво.** [Циклічний зсув](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8932&eid=187827&displayformat=dictionary) слова *x* вліво на *y* бітів позначається *x*<<<*y*. Обернена операція є циклічним зсувом слова *x* вправо на *y* бітів і позначається *x*>>>*y*.

[**Шифрування**](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8932&eid=187834&displayformat=dictionary)[**RC5**](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8932&eid=187748&displayformat=dictionary)**.**

Вхідні дані: [відкритий текст](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8932&eid=187760&displayformat=dictionary) M=(A,B) довжиною 2*w* бітів; кількість раундів *r*; ключ *K*=K[0]…K[b-1].

Вихідні дані: шифрований текст С довжиною 2*w* бітів.

1.     Обчислити (2r+2) підключів S[0]…S[2r+1] за відповідним алгоритмом з вхідного *K* та *r*.

2.     A:=A+S[0], B:=B+S[1] (додавання здійснюється за модулем 2*w*).

3.     **For** *i*=1 **to** *r* **do**: A:=((AB)<<<B)+S[2i], B:=((BA)<<<A)+S[2i+1].

4.     Вихідним значенням є C:=(A,B). (див. рис. 5*а*)

Рис. 5. [Шифрування](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8932&eid=187834&displayformat=dictionary) і [дешифрування](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8932&eid=187765&displayformat=dictionary) [RC5](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8932&eid=187748&displayformat=dictionary).

Входом процесу блокового [шифрування](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8932&eid=187834&displayformat=dictionary) є розширена таблиця ключів S, кількість раундів r, вказівник на вхідний буфер in, та вказівник на вихідний буфер out. Заголовок процедури мовою С, наприклад, може виглядати наступним чином:

*void*[*RC5*](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8932&eid=187748&displayformat=dictionary)*\_Block\_Encrypt (S, r, in, out)*

[*RC5*](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8932&eid=187748&displayformat=dictionary)*\_WORD    \*S;*

*int  r;*

*char    \*in;*

*char    \*out;*

Для початкового завантаження даних слід перетворити вхідні байти на дві беззнакові цілі змінні А та В. Якщо [RC5](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8932&eid=187748&displayformat=dictionary) використовується як 64-бітовий блочний шифр, А та В є 32-бітовими значеннями. Перший байт входу стає найменш значущим байтом А, четвертий байт входу стає найбільш значущим байтом А, п'ятий байт входу стає найменш значущим байтом В і останній байт входу стає найбільш значущим байтом В. Це перетворення найбільш ефективно для процесорів з прямим порядком бітів у байті (little-endian), таких як процесори Intel. Код мовою С для такого перетворення може виглядати, наприклад, так:

*int  i;*

[*RC5*](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8932&eid=187748&displayformat=dictionary)*\_WORD    A, B;*

*A = in[0] & 0xFF;*

*A += (in[1] & 0xFF) << 8;*

*A += (in[2] & 0xFF) << 16;*

*A += (in[3] & 0xFF) << 24;*

*B = in[4] & 0xFF;*

*B += (in[5] & 0xFF) << 8;*

*B += (in[6] & 0xFF) << 16;*

*B += (in[7] & 0xFF) << 24;*

Останнім кроком є перетворення А та В у послідовність байтів. Ця операція є оберненою до операції завантаження. Мовою С це можна, наприклад, представити як:

*out[0] = (A >> 0) & 0xFF;*

*out[1] = (A >> 8) & 0xFF;*

*out[2] = (A >> 16) & 0xFF;*

*out[3] = (A >> 24) & 0xFF;*

*out[4] = (B >> 0) & 0xFF;*

*out[5] = (B >> 8) & 0xFF;*

*out[6] = (B >> 16) & 0xFF;*

*out[7] = (B >> 24) & 0xFF;*

*return;*

[**Дешифрування**](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8932&eid=187765&displayformat=dictionary)[**RC5**](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8932&eid=187748&displayformat=dictionary)**.**

Для [дешифрування](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8932&eid=187765&displayformat=dictionary) використовуються ті самі підключі, які застосовуються для шифрованого тексту C=(A,B) наступним чином (віднімання здійснюється за модулем 2*w*).

1.     **For** *i*=*r* **downto** 1 **do**: B:=((B-S[2i+1])>>>A)A, A:=((A-S[2i])>>>B)B.

2.     Результат M:=(A-S[0],B-S[1]). (рис. 5*б*)

**Створення підключів**[**RC5**](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8932&eid=187748&displayformat=dictionary)**.**

На рис. 6 показана схема обчислення підключів. Підключі зберігаються в масиві з (2*r*+2) слів, елементи якого позначені S[0], S[1],…,S[2r+1]. Використовуючи в якості вхідних даних параметри r та w, цей масив ініціалізується псевдовипадковими фіксованими значеннями. Потім ключ K[0…*b*-1] довжиною *b* байтів перетворюється в масив L[0…*c*-1], що містить *c* слів. Для цього байти ключа копіюються в масив L доповнюючи при необхідності останнє слово справа нулями. Зрештою виконується деяка операція змішування, що об'єднує вміст L з ініціалізованими значеннями S, в результаті чого отримують остаточне значення масиву S.

Рис. 6. Розгортання ключа [RC5](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8932&eid=187748&displayformat=dictionary).

Алгоритм створення підключів виглядає наступним чином:

Вхідні дані: розмір слова в бітах *w*; кількість раундів *r*; ключ довжиною *b* байтів K[0]…K[*b*-1].

Вихідні дані: підключі S[0]…S[2r+1] (де кожне S[i] має довжину *w* бітів).

1.     Перетворення ключа К в масив L. Нехай *u*=*w*/8 (кількість байтів у слові) і *c*=int[*b*/*u*] (довжина К в словах).

Ключ К заповнюється справа нулями при необхідності отримати кількість байтів, що ділиться на *u* (тобто **for** j=*b* **to** (*c**u*-1) **do**: K[j]:=0).

**For** i=0 **to** c-1 **do**:  (тобто заповнюємо L[j] від молодшого до старшого байта використовуючи по одному разу кожен байт K[]).

2.     Ініціалізація масиву S:

S[0]:=*Pw*; **for** i=1 **to** 2r+1 **do**: S[i]:=S[i-1]+*Qw*. (тут *Pw* *Qw* є константами, заснованими на двійковому представленні чисел *е* та  (основи натуральних логарифмів та відношення золотого перетину). Значення цих констант для алгоритму [RC5](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8932&eid=187748&displayformat=dictionary) наведено в табл. 4.)

3.     Змішування ініціалізованого масиву S з масивом ключів L:

i:=0, j:=0, A:=0, B:=0, t:=max(*c*, 2*r*+2).

**For** s=1 **to** 3t **do**: (здійснюється три проходи більшого з масивів L і S)

S[i]:=(S[i]+A+B)<<<3, A:=S[i], i:=(i+1)mod(2*r*+2).

L[j]:=(L[j]+A+B)<<<(A+B), B:=L[j], j:=(j+1)mod(c)

4.     Виходом є S[0], S[1], … , S[2r+1].

При створенні програмного забезпечення захисту інформації особливу увагу слід приділяти безпечній реалізації таких програм. Так, наприклад, основними операціями з ключами [шифрування](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8932&eid=187834&displayformat=dictionary) є створення, знищення та встановлення значення. З метою запобігання розповсюдження ключової інформації в інші частини програми, операція знищення повинна заповнити нулями область пам'яті виділену для роботи з ключем, перед тим як звільняти її менеджеру пам'яті. В загальному об'єкт ключа може підтримувати й інші операції, такі як створення нового випадкового ключа чи отримання ключа з даних протоколу обміну ключами.

Таблиця 4. Константи алгоритму [RC5](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8932&eid=187748&displayformat=dictionary) (у шістнадцятковому вигляді)

|  |  |  |  |
| --- | --- | --- | --- |
| ***w*** | 16 | 32 | 64 |
| ***Pw*** | B7E1 | B7E15163 | B7E15162     8AED2A6B |
| ***Qw*** | 9E37 | 9E3779B9 | 9E3779B9     7F4A7C15 |

Для створення ключа необхідно виділити та ініціалізувати область пам'яті для об'єкту ключа. В наступному прикладі коду мовою С передбачається, що функція з назвою "malloc" повертає блок ініціалізованої пам'яті з кучі, або нуль, що означає помилку.

[*rc5*](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8932&eid=187748&displayformat=dictionary)*UserKey \**[*RC5*](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8932&eid=187748&displayformat=dictionary)*\_Key\_Create ()*

*{*

[*rc5*](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8932&eid=187748&displayformat=dictionary)*UserKey \*pKey;*

*pKey = (*[*rc5*](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8932&eid=187748&displayformat=dictionary)*UserKey \*) malloc (sizeof(\*pKey));*

*if (pKey != ((*[*rc5*](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8932&eid=187748&displayformat=dictionary)*UserKey \*) 0))*

*{*

*pKey->keyLength = 0;*

*pKey->keyBytes = (unsigned char \*) 0;*

*}*

*return (pKey);*

*}*

Для знищення ключа пам'ять повинна бути заповнена нулями та звільнена менеджеру пам'яті. В наступному прикладі коду мовою С передбачається, що функція з назвою "free" повертає блок пам'яті в кучу.

*void*[*RC5*](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8932&eid=187748&displayformat=dictionary)*\_Key\_*[*Des*](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8932&eid=187737&displayformat=dictionary)*troy (pKey)*

[*rc5*](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8932&eid=187748&displayformat=dictionary)*UserKey      \*pKey;*

*{*

*unsigned char   \*to;*

*int          count;*

*if (pKey == ((*[*rc5*](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8932&eid=187748&displayformat=dictionary)*UserKey \*) 0))*

*return;*

*if (pKey->keyBytes == ((unsigned char \*) 0))*

*return;*

*to = pKey->keyBytes;*

*for (count = 0 ; count < pKey->keyLength ; count++)*

*\*to++ = (unsigned char) 0;*

*free (pKey->keyBytes);*

*pKey->keyBytes = (unsigned char \*) 0;*

*pKey->keyLength = 0;*

*free (pKey);*

*}*

Двома найбільш важливими особливостями [RC5](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8932&eid=187748&displayformat=dictionary) є простота алгоритму та використання керованих даними циклічних зсувів. Циклічні зсуви – єдина нелінійна складова даного алгоритму. Райвест стверджує, що, у зв'язку з тим, що величина зсуву визначається даними, що обробляються алгоритмом, лінійний та диференційний [криптоаналіз](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8932&eid=187777&displayformat=dictionary) алгоритму буде серйозно утруднений.

**Режими**[**RC5**](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8932&eid=187748&displayformat=dictionary)**.**

З метою забезпечення можливості ефективного використання [RC5](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8932&eid=187748&displayformat=dictionary) в неоднорідному середовищі, специфікація RFC 2040 визначає чотири різних режими роботи цього алгоритму.

        [**Блоковий шифр**](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8932&eid=187758&displayformat=dictionary)[**RC5**](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8932&eid=187748&displayformat=dictionary)**.** Алгоритм прямого [шифрування](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8932&eid=187834&displayformat=dictionary), при якому береться блок даних заданого розміру (2*w* бітів) і з нього за допомогою залежного від ключа перетворення генерується блок шифрованого тексту такого самого розміру (див. рис. 7). Цей режим часто називають режимом [ECB](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8932&eid=187740&displayformat=dictionary) (режим електронної шифрувальної книги).

        **RC5-CBC.** Режим зв'язаних шифрованих блоків для [RC5](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8932&eid=187748&displayformat=dictionary) (рис. 8). В режимі СВС обробляються повідомлення, довжина яких кратна розміру блока [RC5](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8932&eid=187748&displayformat=dictionary) (тобто кратна 2*w* бітам). Режим СВС забезпечує вищий ступінь захисту, ніж ЕСВ, оскільки генерує різні блоки шифрованого тексту для однакових повторних блоків відкритого тексту.

        **RC5-CBC-Pad.** [Модифікація](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8932&eid=187792&displayformat=dictionary) режиму СВС, призначена для роботи з відкритим текстом будь-якої довжини. Довжина шифрованого тексту в цьому режимі перевищує довжину відкритого тексту не більш ніж на довжину одного блоку [RC5](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8932&eid=187748&displayformat=dictionary).

        **RC5-CTS.** Режим запозичення шифрованого тексту (ciphertext stealing), теж є модифікацією СВС. В цьому режимі допускається обробка відкритого тексту будь-якої довжини і генерується шифрований текст тієї самої довжини.

Рис. 7. Режим електронної шифрувальної книги.

Режим зв’язаних шифрованих блоків (Cipher Block Chaining – CBC) забезпечує вищий ступінь захисту ніж режим електронної шифрувальної книги (Electronic Codebook – [ECB](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8932&eid=187740&displayformat=dictionary)), в якому кожен блок відкритого тексту шифрується незалежно, оскільки генерує різні блоки шифрованого тексту для однакових блоків відкритого тексту, які повторюються в повідомленні. В режимі CBC (рис. 8) вхідне значення алгоритму [шифрування](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8932&eid=187834&displayformat=dictionary) дорівнює результату операції [XOR](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8932&eid=187752&displayformat=dictionary) поточного блоку відкритого тексту і отриманого на попередньому кроці блоку шифрованого тексту. [Шифрування](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8932&eid=187834&displayformat=dictionary) будь-якого блоку виконується за допомогою одного і того ж ключа. В результаті в процесі [шифрування](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8932&eid=187834&displayformat=dictionary) усі блоки відкритого тексту виявляються зв'язаними, а вхідні дані, що поступають на вхід функції [шифрування](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8932&eid=187834&displayformat=dictionary), вже не жорстко зв'язані з блоками відкритого тексту. Тому однакові блоки відкритого тексту перетворюються в різні блоки шифрованого тексту.

При дешифруванні текст також проходить через алгоритм [дешифрування](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8932&eid=187765&displayformat=dictionary) поблочно. При цьому відповідний блок відкритого тексту отримується як результат операції XOR вихідного блоку алгоритму [дешифрування](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8932&eid=187765&displayformat=dictionary) і попереднього блоку шифрованого тексту. У вигляді формули цей режим можна записати як:

.

Тут *EK* і *DK* означає операцію [шифрування](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8932&eid=187834&displayformat=dictionary) ([дешифрування](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8932&eid=187765&displayformat=dictionary)) з ключем *К*, *Ci* та *Pi* – *і*-й блок шифрованого та відкритого тексту відповідно, а знак  позначає операцію побітового виключного АБО ([XOR](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8932&eid=187752&displayformat=dictionary)).

Тоді

, а

.

Щоб отримати перший блок шифрованого тексту, розглядається результат операції [XOR](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8932&eid=187752&displayformat=dictionary) деякого вектора ініціалізації (IV) і першого блоку відкритого тексту. При дешифруванні для відновлення першого блоку відкритого тексту необхідно буде також виконати операцію [XOR](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8932&eid=187752&displayformat=dictionary) по відношенню до цього вектора IV і першого блоку на виході алгоритму [дешифрування](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8932&eid=187765&displayformat=dictionary).

Рис. 8. Режим зв’язаних шифрованих блоків.

Значення IV повинно бути відомим і відправнику і отримувачу повідомлення. Для забезпечення максимальної безпеки значення IV повинно бути захищено так само, як і ключ [шифрування](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8932&eid=187834&displayformat=dictionary). Можна, наприклад, відправити значення IV зашифроване в режимі [ECB](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8932&eid=187740&displayformat=dictionary). Документ RFC 2040 передбачає в якості значення за замовчуванням рядок відповідної довжини, що складається з нульових байтів.

Коли [шифрування](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8932&eid=187834&displayformat=dictionary) повідомлення проводиться в режимі CBC, необхідний деякий алгоритм підготовки до [шифрування](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8932&eid=187834&displayformat=dictionary) повідомлень, довжина яких не кратна довжині блоку. Одним з таких методів для алгоритму [шифрування](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8932&eid=187834&displayformat=dictionary) [RC5](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8932&eid=187748&displayformat=dictionary) є режим [RC5](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8932&eid=187748&displayformat=dictionary)-CBC-Pad. В цьому режимі, при підготовці до [шифрування](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8932&eid=187834&displayformat=dictionary) повідомлень, довжина яких не кратна довжині блоку, використовується заповнювач для доповнення повідомлення до потрібної довжини. В результаті довжина шифрованого тексту в цьому режимі перевищує довжину відкритого тексту не більше ніж на довжину одного блоку [RC5](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8932&eid=187748&displayformat=dictionary). В алгоритмі [RC5](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8932&eid=187748&displayformat=dictionary) вважається, що будь-яке повідомлення складається з цілої кількості байтів. В кінець повідомлення додається від 1 до *bb* байтів заповнювача[[1]](http://vns.lp.edu.ua/mod/page/view.php?id=189885" \l "_ftn1" \o "), де *bb* дорівнює довжині блоку [RC5](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8932&eid=187748&displayformat=dictionary) в байтах (*bb*=2*w*/8). Усі байти заповнювача вибираються однаковими і рівними значенню кількості доданих байтів. Наприклад, якщо додається 8 байтів, то кожен байт вибирається рівним 00001000.

**Завдання до виконання роботи**

Згідно до варіанту, наведеного в таблиці, створити прикладну програму для [шифрування](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8932&eid=187834&displayformat=dictionary) інформації за алгоритмом [RC5](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8932&eid=187748&displayformat=dictionary).

Програма повинна отримувати від користувача парольну фразу і, на її основі, шифрувати файли довільного розміру, а результат зберігати у вигляді файлу з можливістю подальшого [дешифрування](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8932&eid=187765&displayformat=dictionary) (при введенні тієї самої парольної фрази).

Для перетворення парольної фрази у ключ [шифрування](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8932&eid=187834&displayformat=dictionary) використати алгоритм [MD5](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8932&eid=187743&displayformat=dictionary), реалізований в лабораторній роботі № 2 – ключем [шифрування](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8932&eid=187834&displayformat=dictionary) повинен бути хеш парольної фрази. Якщо згідно варіанту довжина ключа становить 64 біти, беруться молодші 64 біти хешу; якщо довжина ключа повинна бути 256 бітів, то хеш парольної фрази стає старшими 128 бітами, а молодшими є хеш від старших 128 бітів (тобто, позначивши парольну фразу через *P*, отримаємо *K*=*H*(*H*(*P*))||*H*(*P*)).

Для забезпечення можливості роботи створеного програмного продукту з відкритим текстом довільної довжини, програмну реалізацію здійснити в режимі [RC5](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8932&eid=187748&displayformat=dictionary)-CBC-Pad. В якості вектора ініціалізації (IV) використати [генератор псевдовипадкових чисел](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8932&eid=187762&displayformat=dictionary), реалізований в лабораторній роботі № 1. Для кожного нового шифрованого повідомлення слід генерувати новий вектор ініціалізації. Вектор ініціалізації зашифровується в режимі [ECB](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8932&eid=187740&displayformat=dictionary) і зберігається в першому блоці зашифрованого файлу.

У звіті навести протокол роботи програми та зробити висновки про поєднання різних криптографічних примітивів для задач захисту інформації.

Варіанти для виконання лабораторної роботи:

|  |  |  |  |
| --- | --- | --- | --- |
| № варіанту | *Довжина слова (w)*, біт | *Кількість раундів (r)* | *Довжина ключа (b)*, байт |
| 1. | 16 | 8 | 16 |
| 2. | 32 | 12 | 16 |
| 3. | 64 | 16 | 32 |
| 4. | 16 | 20 | 16 |
| 5. | 32 | 8 | 32 |
| 6. | 64 | 12 | 8 |
| 7. | 16 | 16 | 8 |
| 8. | 32 | 20 | 16 |
| 9. | 64 | 8 | 32 |
| 10. | 16 | 12 | 16 |
| 11. | 32 | 16 | 8 |
| 12. | 64 | 20 | 16 |
| 13. | 16 | 8 | 32 |
| 14. | 32 | 12 | 32 |
| 15. | 64 | 16 | 16 |
| 16. | 16 | 20 | 8 |
| 17. | 32 | 8 | 8 |
| 18. | 64 | 12 | 16 |
| 19. | 16 | 16 | 32 |
| 20. | 32 | 20 | 32 |
| 21. | 64 | 8 | 16 |
| 22. | 16 | 12 | 8 |
| 23. | 32 | 16 | 32 |
| 24. | 64 | 20 | 8 |
| 25. | 16 | 8 | 8 |

**Контрольні запитання.**

1.     Для яких задач використовуються алгоритми симетричного [шифрування](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8932&eid=187834&displayformat=dictionary)?

2.     Якими параметрами визначається алгоритм [RC5](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8932&eid=187748&displayformat=dictionary)?

3.     Яка довжина ключа [шифрування](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8932&eid=187834&displayformat=dictionary) алгоритму RC5?

4.     Які елементарні операції використовуються в алгоритмі [RC5](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8932&eid=187748&displayformat=dictionary)?

5.     Які операції є нелінійними функціями алгоритму [шифрування](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8932&eid=187834&displayformat=dictionary) [RC5](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8932&eid=187748&displayformat=dictionary)?

6.     Які режими роботи передбачені для алгоритму [шифрування](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8932&eid=187834&displayformat=dictionary) [RC5](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8932&eid=187748&displayformat=dictionary)?

7.     Який режим роботи алгоритму [RC5](http://vns.lp.edu.ua/mod/glossary/showentry.php?courseid=8932&eid=187748&displayformat=dictionary) слід використати якщо довжина шифрованого тексту повинна дорівнювати довжині довільного відкритого тексту?