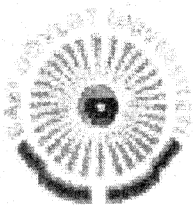
MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE
ACADEMY OF PEDAGOGICAL SCIENCES OF UKRAINE
VINNYTSIA NATIONAL TECHNICAL UNIVERSITY
"STEFAN cel MARE" UNIVERSITY of SUCEAVA
BAKU STATE UNIVERSITY
NATIONAL INFORMATION CENTRE FOR
UKRAINE-EU SCIENCE AND TECHNOLOGY COOPERATION




PROCEEDINGS

of the Fifth International Conference

INTERNET - EDUCATION – SCIENCE

IES – 2006

Volume 2

10-14 October, 2006 *Vinnytsia - UKRAINE*

UNIVERSUM-VINNYTSIA
2006

УДК 378 + 681.324
І73

Друкується за рішенням Ученої ради Вінницького національного технічного університету Міністерства освіти і науки України

Відповідальний за випуск *В. В. Грабко*
Підготовлено до друку: *В. В. Грабко, В. І. Месюра, О. А. Дячок*

І 73 **ІНТЕРНЕТ-ОСВІТА-НАУКА-2006, п'ята міжнародна конференція ІОН–2006**, 10–14 жовтня, 2006. Збірник матеріалів конференції. Том 2. – Вінниця: УНІВЕРСУМ-Вінниця, 2006. – 420 с.

ISBN 966-641-193-8 (том 2)

П'ята міжнародна конференція "ІНТЕРНЕТ – ОСВІТА – НАУКА – 2006" (ІОН –2006) присвячена обговоренню питань застосування в освіті та наукових дослідженнях нових інформаційних технологій, що спираються на можливості Інтернет.

УДК 378 + 681.324

Доповіді у збірнику згруповані по секціях, відповідно до основних напрямків конференції:

Том1:

A Інтернет та інформаційні технології в освіті та наукових дослідженнях
B Методологія та практика дистанційної освіти
C Психологія кіберпростору
D Інформаційні технології в економіці
E Програмне забезпечення для Інтернет

Том2:

F Комп'ютерні мережі та захист інформації
G Технології обробки та передачі зображень
H Інтелектуальні інформаційні системи
I Комп'ютерне моделювання у наукових дослідженнях

Матеріали доповідей також представлені на Web-сайті конференції (http:/www.vstu.vinnica.ua/ies2006), що містить електронну версію даного збірника, і базу даних з відомостями про учасників конференції.

Тексти доповідей друкуються в авторській редакції.

ISBN 966-641-191-1 (загальний)

ISBN 966-641-193-8 (том 2)

ШИФРУВАННЯ ДАНИХ ІМОВІРНІСНИМ МЕТОДОМ

Володимир Майданюк, Валентина Каплун

Вінницький національний технічний університет
Хмельницьке шосе, 95, Вінниця, 21021, Україна, Тел.: (0432) 59-83-70, E-mail: nach@lib.vstu.edu.ua

Abstract

In the given article the questions of the use of algorithms of compression without the losses for enciphering of data are examined. Some statistical algorithms of compression without the losses are characterized to those, that before the beginning of compression the table of characters is formed. The code after the degree of newness belongs to such algorithms, probabilistic code et al. Therefore if to form this table of characters with the use of generator of pseudorandom numbers, for example, with an initial number as a key of code, actually at the compression, enciphering is simultaneously executed. In work the results of research of the use of probabilistic method of compression are resulted for enciphering.

Вступ

Більшість сучасних операційних систем, прикладних пакетів обробки електронних документів, починаючи з найпростіших і до самих складних, обов'язково містять у собі функції захисту оброблюваної інформації від несанкціонованого (стороннього) доступу і зміни. Як правило, ці функції втілюють ті чи інші алгоритми захисту документів від підробки. Тому, можна впевнено говорити, що ці функції в будь-якій сучасній автоматизованій інформаційній системі є її важливими і невід'ємними частинами.

Проблемами захисту інформації займається криптологія (kryptos - таємний, logos - наука). Криптологія розділяється на два напрямки - криптографію і криптоаналіз. Мета цих двох напрямків криптології прямо протилежна [1-3].

Криптографія - наука про захист інформації від несанкціонованого доступу до неї сторонніх осіб.

Д.Кан називає криптографією мистецтво зберігати інформацію в секреті. Згідно з Кобліцем та Конхеймом криптографія – це мистецтво та наука зробити інформацію що передається доступною лише для даного одержувача.

Криптографія стала формуватися як самостійна наука із широким поширенням писемності. Перші криптосистеми зустрічаються вже на початку нашої ери. Так, Юлій Цезар у своєму переписуванні із Цицероном використовував уже більш менш систематичний шифр, що одержав його ім'я. Його шифр реалізувався шляхом заміни кожної букви в повідомленні іншою буквою того ж алфавіту, але віддаленої від неї на фіксоване число позицій.

Бурхливий розвиток криптографічні системи одержали в роки першої і другої світових воєн. Починаючи з післявоєнного часу і по нинішній день поява обчислювальних засобів прискорила розробку і удосконалення криптографічних методів.

Проблема використання криптографічних методів в інформаційних системах стала найбільш актуальною проблемою сьогодення тому, що по-перше розширилося використання комп'ютерних мереж, зокрема глобальної мережі Інтернет, по яких передаються великі обсяги інформації державного, військового, комерційного і приватного характеру, що не допускає можливість доступу до неї сторонніх осіб.

Захищена інформаційна система повинна протистояти атакам зі сторони порушника. Тому криптографія займається розробкою і дослідженням методів шифрування інформації, щоб унеможливити, або зробити досить трудомісткім процес розшифрування.

Шифрування - перетворення інформації, у результаті якого вихідний текст (відкритий текст) заміняється закритим (шифрованим) текстом, тобто шифрограмою.

Дешифрування - зворотний шифруванню процес. На основі ключа зашифрований текст (шифрограма, шифровка) перетворюється у вихідний відкритий текст.

Сфера інтересів криптоаналізу протилежна - розробка і дослідження методів дешифрування (розкриття) шифрограми навіть без знання секретного ключа.

Під ключем розуміється секретна інформація, що визначає, яке перетворення виконується в даному випадку над відкритим текстом.

Процес одержання криптоаналітиками відкритого повідомлення із шифрованого повідомлення без заздалегідь відомого ключа називається розкриттям або зломом шифру.

Отже, криптографія дає можливість перетворити інформацію таким чином, щоб її прочитання (відновлення) було можливим лише при наявності ключа. В своїй відомій роботі "Теорія зв'язку в секретних системах" (1949р.) К.Шеннона показав, що ущільнення даних може значно збільшити криптостійкість алгоритму шифрування навіть для коротких ключів. Однак донедавна алгоритми ущільнення даних [4-5] і криптографічного захисту розвивались окремо, що приводило до значних обчислювальних витрат, оскільки при передачі і зберіганні файлів виникає необхідність в подвійному