УДК 681.3.07

І. Д. ГОРБЕНКО, д-р техн. наук, О. А. МЕЛЬНИКОВА, канд.техн. наук, І. Г. ОСТАПЕНКО

ДОСВІД ПІДГОТОВКИ ТА РЕЗУЛЬТАТИ ПРОВЕДЕННЯ V ВСЕУКРАЇНСЬКОЇ ОЛІМПІАДИ В НАПРЯМКУ «ІНФОРМАЦІЙНА БЕЗПЕКА»

На базі Харківського національного університету радіоелектроніки у квітні 2003 року проводився другий тур V Всеукраїнської студентської олімпіади з напрямку «Інформаційна безпека» серед студентів III – V курсів університетів та технічних ВУЗів України. Олімпіада проводилася за двома рівнями складності. Перший рівень – для студентів III – V курсів та магістрів зі спеціальностей напрямку «Інформаційна безпека», другий рівень – для студентів III – V курсів та магістрів, що вивчають загальноосвітні та прикладні дисципліни з захисту інформації.

Олімпіада проводилась в два тури. Перший тур був пов'язаний з розв'язком задач різної складності та реалізації однієї задачі у вигляді програмного продукту. При оцінці розробленої програми враховувалася як правильність її функціонування, так і якість реалізації (наприклад, характеристики швидкості, пам'яті, повнота проведеного тестування і т.і.). Додатково на Олімпіаді проводився другий тур, який мав вигляд презентації та захисту власних проектів та розробок за напрямком «Інформаційна безпека», у тому числі статей, патентів, програмних продуктів, апаратних засобів, тощо. Цей тур здійснювався у вигляді стендової комп'ютерної доповіді.

Цього року в олімпіаді приймали участь такі ВУЗи: Національний технічний університет України «Київський політехнічний інститут»- 3 чол; Національний гірничий університет м. Дніпропетровськ – 2 чол.; Національний авіаційний університет, м. Київ – 2 чол; Криворізький технічний університет – 2 чол.; Дніпропетровський національний університет – 3 чол.; Сумський державний університет – 1 чол.; Тернопільська академія народного господарства – 2 чол.; Львівський національний університет ім. І. Франка – 1 чол.; Український державний морський технічний університет, м. Миколаїв – 4 чол.; Харківський національний університет радіоелектроніки – 10 чол.; Харківський інститут військово-повітряних сил – 5 чол.; Національний технічний університет «Харківський політехнічний інститут» – 2 чол.

1 Конкурсні завдання

Цього року повністю оновленні конкурсні завдання, змінено підхід до формування завдань.

Конкурсні завдання з напряму «Інформаційна безпека»

Задача № 1 (12 балів).

В радіомережі зв'язку для забезпечення конфіденційності n абонентів використовують безумовно стійкий шифр Вернама з гамуванням за модулем 2. Ключові дані формуються центром генерації на основі випадкових чисел. Абоненти обмінюються між собою короткими повідомленнями з довжиною l бітів та інтенсивністю r повідомлень за добу.

Чи можливі колізії ключів в такій системі та в чому їх загрозливість?

Знайдіть імовірність колізії хоч би двох ключів на протязі доби, якщо

$$l = 48 + k, \quad n = 2^{4+t}, \quad r = 2^{6+t}, \quad t \equiv k(\mathrm{mod}\,7)$$

де k – номер реєстрації учасника олімпіади.

Задача № 2 (12 балів).

Лазерні прибори дистанційної розвідки мовної звукової інформації працюють за рахунок коливань віддзеркалюючи поверхнею, наприклад, шибок вікон.

Оцінити амплітуду коливань середини одинарної шибки вікна під дією звукового тиску p=1Па гармонічного коливання частотою f=1кГц при слідуючи умовах і припущеннях.

Величина звукоізоляції згаданої шибки R=20дБ.

Звукоізоляція розраховується за формулою

$$R = 10\lg(p_1/p_2)^2$$

де $p1$ – звуковий тиск перед шибкою вікна,

$p2$ – звуковий тиск за шибкою вікна.

Для хвиль у повітрі діє відоме співвідношення

$$p=vrc,$$

де v – швидкість руху молекул повітря під дією звукових хвиль,

r – густина повітря,

c – швидкість розповсюдження звукових хвиль у повітрі.

Для нормальних атмосферних умов $rc = 420$ Н*с/м^3.

Рух молекул повітря за шибкою повністю співпадає із рухом самої шибки.

Задача № 3 (12 балів).

1. Порівняйте перспективи застосування криптоперетворень в кільцях, полях та групах точок еліптичних кривих по критеріям стійкості та складності.
2. Сформуйте пропозиції по застосуванню одного із вказаних криптоперетворень на практиці.
3. Визначте вартість криптоаналізу методом повного розкриття при якому знаходиться особистий ключ, якщо довжини модулів криптоперетворень

$l_i = 256 + k \cdot 8$

при умові, що потужність криптоаналітичної системи в полях та кільцях складає $\gamma_1 = k \cdot 10^{16}$ *груп. оп*$/c$, а в групі точок еліптичної кривої $\gamma_2 = k \cdot 10^{13}$ *додавань*$/c$. Вартість 1 міпсороку складає для криптоперетворень в полях та кільцях 10 грн., а в групі точок ЕК – 30 грн.

Додаткова задача № 4 (10 балів).

В системі криптографічного захисту інформації використовується схема Діффі-Хеллмана відкритого розподілу ключів з загальносистемними параметрами $\{P,\theta\}$, де P – просте число, θ – твірний елемент мультиплікативної групи GF(P). Особисті ключі, які абоненти формують випадково, розподілені на множині {1,2,3,…,P-2,P-1}.

Необхідно:

1. Знайти розподіл на множині загальних секретів (ключів), які використовують абоненти.
2. Знайти розподіл при P=31.

Конкурсні завдання з дисципліни «Захист інформації»

Задача № 1 (12 балів).

В радіомережі зв'язку для забезпечення конфіденційності обміну повідомленнями двох абонентів використовується потокове гамування за модулем 2. Ключі, що визначають реалізацію гами шифруючої формуються випадково і рівно ймовірно.

Знайдіть імовірність перекриття шифру (колізії гам шифруючих) за добу роботи, якщо довжина повідомлень $l = 32 + 2k$ бітів, інтенсивність обміну $r = 2^{8+t}$ повідомлень за добу, а $t = k(\mathrm{mod}\,7)$, k – номер реєстрації учасника олімпіади.

Задача № 2 (12 балів).

Обґрунтуйте перспективи застосування криптографічних перетворень в групі точок еліптичних кривих (ЕК). Назвіть основні додатки, для яких ці перетворення можуть бути використані.

Порівняйте стійкість криптоперетворень в кільці (RSA), полі (Діффі-Хеллмана) та групі точок ЕК, якщо:

- модуль N RSA перетворення $l_N = 768 + k \cdot 32$ бітів,
- модуль P D-H перетворення $l_P = 768 + k \cdot 32$ бітів,
- модуль перетворення n (порядок точки) ЕК $l_n = 192 + k \cdot 8$ бітів.

Визначте безпечний час вказаних криптоперетворень, якщо потужність криптоаналітичної системи

$$\gamma_{RSA} = 10^{10}\ on/c, \quad \gamma_{D-H} = 10^{10}\ on/c, \quad \gamma_{EK} = 10^{8}\ on/c$$

Задача № 3 (12 балів).

Розв'яжіть порівняння

$$15^x = k + 1 (\mathrm{mod}\, 37)$$

де k – номер реєстрації учасника.

Визначте умови існування розв'язання та поясніть можливість застосування даного алгоритму розв'язання при криптоаналізі

Додаткова задача № 4 (10 балів).

Перевірте:

1. Чи являється многочлен $f(x) = x^4 + x + 1$ неприводимим над полем GF(2)?
2. Чи являється $f(x)$ примітивним для розширеного поля GF(2^4)?
3. Яка довжина періоду повторення послідовності, що породжується $f(x)$?
4. Чи породжує $f(x)$ послідовність максимального періоду?

   Назвіть основні властивості послідовності, що формується згідно $f(x)$.

2 Результати олімпіади та аналіз рівня підготовки конкурсантів

Всього в олімпіаді прийняла участь 37 осіб із 12 вузів України. За результатами олімпіади місця розподілилися таким чином.

Переможці з напрямку «Інформаційна безпека»(особистий залік)

1 місце – Торба Сергій Миколайович (НТУУ «КПІ») – 46 балів;
2 місце – Мельник Олександр Іванович (ХНУРЕ) – 45балів;
3місце – Васильєв Іван Володимирович (НТУУ «КПІ») – 43 бали.

Переможці з дисципліни «Захист інформації» (особистий залік)

1 місце – Михайленко Матвей Сергійович (ХНУРЕ) – 45 балів;
2 місце – Бакулін Андрій Олександрович (ХНУРЕ) – 44 бали;
3 місце – Артюхов Олександр Геннадійович (ХНУРЕ) – 43 бали.

Командні переможці з напрямку «Інформаційна безпека»

1 місце команда в складі: Боня Юрій Юрійович, Васильєв Іван Володимирович, Торба Сергій Миколайович (НТУУ «КПІ») – 128 балів;

2 місце команда в складі: Мельник Олександр Іванович, Понамарьов Денис Володимирович, Хижний Андрій Вікторович (ХНУРЕ) – 126 балів;

3 місце команда в складі: Калініченко В'ячеслав Петрович, Іванько Артем Миколайович (НГУ м. Дніпропетровськ) – 58 балів.

Командні переможці з дисципліни «Захист інформації»

1 місце команда в складі: Артюхов Олександр Геннадійович, Михайленко Матвій Сергійович, Бакулін Андрій Олександрович (ХНУРЕ) – 132 бали;

2 місце команда в складі: Зайнулін Костянтин Ігорович, Цимбалюк Олександр Сергійович, Макуха Андрій Володимирович (ХІВПС) – 78 балів;

3 місце команда в складі: Підопригора Павло Олексійович, Дзигін Євгеній Валерійович, Богун Костянтин Олександрович (ДНУ) – 41 бал.

Крім того, були нагороджені:

За оригінальність особистої програмної розробки з напрямку «Інформаційна безпека» – Антонов Артем Вікторович (ХІВПС);

За власний проект експертної системи «Советник» – Леншин Анатолій Валерійович (ХВУ)

До основних недоліків у підготовці конкурсантів слід віднести наступне.

— при вивченні тем, наприклад, симетричних шифрів, студенти поверхово засвоюють алгоритми, не володіють уміннями доводити коректність алгоритмів, використовувати для цього, наприклад, теорію колізій;

— не усі студенти знають критерії та показники, що можуть бути застосовані при порівнянні різних асиметричних алгоритмів (наприклад в кільцях, полях та групах точок еліптичних кривих);

— не достатня, а то і слабка підготовка студентів з питань таких спецрозділів математики, як теорія чисел, теорія груп взагалі, та теорія еліптичних груп частково;

— значна кількість студентів мають слабкі знання з питань технічного захисту інформації, наприклад, з питань лазерного перехоплення інформації через шибки вікон.

Проведена олімпіада підтвердила зрослий рівень підготовленості магістрів та студентів з проблемних питань захисту інформації в напрямку «Інформаційна безпека», вони розуміють основні протиріччя та орієнтуються в напрямках їх розв'язку. Добре підготовлені, в тому числі математично, магістри та студенти НТТУ «КПІ» та ХНУРЕ. Зросла підготовленість студентів Національної гірничої академії. Крім того, студенти цих вузів вільно складають програми та вирішують за їх допомогою складні задачі з використанням ПЕОМ.

В номінації «Захист інформації», в якій виступали студенти других спеціальностей, але такі, що вивчали одну або дві загально освітні дисципліни з захисту інформації, студенти також продемонстрували зрослий рівень знань та умінь. Знають проблемні питання та новітні алгоритми криптографічного захисту інформації. Але математичний рівень підготовки в криптології, на наш погляд, недостатній, крім того, треба формувати краще і їх світогляд.

Харківський національний
університет радіоелектроніки

Надійшла до редколегії 12.05.2003