УДК 681.3.07

І.Д. ГОРБЕНКО, д-р техн. наук, А.В. ПОТІЙ, канд. техн. наук,
О.А. МЕЛЬНИКОВА, канд.техн. наук

ДОСВІД ПІДГОТОВКИ ТА РЕЗУЛЬТАТИ ПРОВЕДЕННЯ IV ВСЕУКРАЇНСЬКОЇ ОЛІМПІАДИ СЕРЕД БАКАЛАВРІВ, СТУДЕНТІВ ТА МАГІСТРІВ З НАПРЯМКУ «ІНФОРМАЦІЙНА БЕЗПЕКА»

Згідно з наказом Міністерства освіти і науки України № 800 від 13.12.2001 р. "Про проведення Всеукраїнської студентської олімпіади 2001 - 2002" на базі Харківського Національного університету радіоелектроніки у квітні 2002 року проводився другий етап всеукраїнської студентської олімпіади з напрямку "Інформаційна безпека" серед студентів III - V курсів університетів та технічних ВУЗів України. Олімпіада проводилася по двом рівням 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 в вигляді програмного продукту. Всього для розв'язку було запропоновано 7 теоретичних задач, 3 з яких по складності відповідають першому рівню, а 4 — другому рівню. За правильний розв'язок кожної задачі, в залежності від складності, призначалося від 5 до 12 балів. А також були запропоновані варіанти практичних завдань для програмної реалізації. 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 по напрямку "Інформаційна безпека", в тому числі статей, патентів, програмних продуктів, апаратних засобів тощо. Цей тур здійснювався в вигляді стендової комп'ютерної доповіді.

Цього року в олімпіаді приймали участь наступні ВУЗи: Національний технічний університет України "КПІ" (м. Київ) — 4 чол., Українська академія банківської справи Харківської філії (м. Харків) — 1 чол., Харківський національний політехнічний університет "ХПІ" — 2 чол., Сумський Державний університет (м. Суми) — 2 чол., Харківський інститут Військово - Повітряних сил — 5 чол., Волинський державний університет ім. Лесі Українки — 1 чол., Харківський національний університет радіоелектроніки — 9 чол., Національна юридична академія України ім. Ярослава Мудрого — 1 чол., Дніпропетровський національний горний університет України — 2 чол., Дніпропетровський національний університет фізико технічний інститут — 2 чол.

1. Конкурсні завдання

Цього року було змінено підхід до формування завдань та повністю оновлено набори конкурсних завдань. Для прикладу нижче наведемо використаний набір конкурсних завдань. Завдання 1 - 4 були призначені для напрямку "Інформаційна безпека", завдання 4 – 7 — для спеціальності "Захист інформації в системах та мережах".

Завдання № 1 (12 балів). В системі захисту інформації для забезпечення цілісності використовується однонаправлена хеш - функція $H(M) = h$, де M — інформація довільної довжини, а h може приймати $n = 2^m$ значень. Скільки випадкових повідомлень k необхідно подати на вхід перетворювача H, щоб з імовірністю $P_з$ відбулося хоча б одне співпадання вигляду $H(M_i) = H(M_j)$, тобто відбулася колізія. Визначити конкретне значення k для відомої Вам хеш - функції, якщо $P_з = 0{,}5 + i \cdot 0{,}02$, де i — номер реєстрації учасника олімпіади. При $i > 25$ $i := i \pmod{25}$.

Завдання № 2 (12 балів). В стандарті США X9.30 цифровий підпис $< r, S >$ формується згідно наступних правил

$$\begin{cases} r = g^k \pmod P \bmod q \\ S = \left[k^{-1} \cdot \left(h(M) + x \cdot r\right)\right] \bmod q \end{cases} \quad (1)$$

Для повідомлення $[M', < r', S' >]$ перевірка підпису здійснюється в наступній послідовності

$$W = (S')^{-1} \bmod q \quad (2)$$

$$U_1 = [H(M') \cdot W] \bmod q \quad (3)$$

$$U_2 = (r') \cdot W \bmod q \quad (4)$$

$$V = \left[\left(g^{U_1} \cdot y^{U_2}\right) \bmod p\right] \bmod q \quad (5)$$

де x — особистий ключ цифрового підпису, g — первісний елемент, P, q — великі прості числа, причому q входить в канонічний розклад P - 1 як співмножник, $H(M)$ — функція хешування, y — відкритий ключ. Доведіть, що повідомлення M' буде цілісним та справжнім, якщо $V = r$.

Визначте складність криптоаналізу методом розв'язку дискретного логарифмічного порівняння, якщо $P_i = 2^{512+i\cdot 64}$, $i := i \pmod 8$, де i — номер реєстрації учасника олімпіади.

Як та на яку величину зміниться стійкість, якщо замість DSA використати ECDSA (підпис на еліптичних кривих) з порядком базової точки G дорівнюючим $n_i = P_i$.

Завдання № 3 (12 балів). Монохроматичний монітор ПЕОМ з діагоналлю 17′ підтримує (забезпечує) 1024·168 елементів зображення. Частота кадрів 80 Гц. Амплітуда імпульсів вихідного каскаду, що подаються на катод електронної променевої трубки (ЕПТ) 200 В, 10 мА. Зворотний хід рядкової та кадрової розгортки займає 18% та 8% відповідних періодів. Необхідно виконати наступні підпункти завдання.

– Намалювати (якісно) вигляд спектру амплітуд сигналу у колі монітора.

– Як буде змінюватись спектр амплітуд сигналу у колі при зміні фронтів імпульсу від прямокутного до косинус - квадратичного з різною протяжністю ? Навести на малюнку якісні зміни. Як це буде впливати на фактори ТЗІ ?

– Як зміниться спектр при застосуванні монітора з діагоналлю 21′ ?

– Які елементи конструкції монітора впливають на інтенсивність випромінювання сигналу монітора.

Завдання № 4 (12 балів). У федеральному стандарті симетричного шифрування США 21 століття FIPS - 197 для перемішування та розсіювання використовуються два табличні перетворення: заміна байтів та зсув байтів рядків.

Заміна байтів здійснюється спочатку послідовною заміною кожного a_{ij} байту стану на зворотній a_{ij}^{-1} згідно порівняння

$$a_{ij} \cdot a_{ij}^{-1} \equiv 1 \left(\bmod x^8 + x^4 + x^3 + x + 1\right). \quad (6)$$

Потім кожен $a_{ij}^{-1} = x$ байт замінюється на Y згідно ниженаведенного афінного перетворення

$$Y = \begin{vmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \\ y_7 \end{vmatrix} = \begin{vmatrix} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{vmatrix} \times \begin{vmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{vmatrix} \oplus \begin{vmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \end{vmatrix} \quad (7)$$

Зсув рядків байтів плинного стану A_V

$$A_V = \begin{vmatrix} a_{00} & a_{01} & a_{02} & a_{03} \\ a_{10} & a_{11} & a_{12} & a_{13} \\ a_{20} & a_{21} & a_{22} & a_{23} \\ a_{30} & a_{31} & a_{32} & a_{33} \end{vmatrix} \quad (8)$$

здійснюється циклічно зліва направо згідно наступних правил: перший рядок без зсуву, другий на один байт, третій на 2 байти, четвертий на 3 байти. Необхідно виконати наступні пункти завдання.

– Довести, що перетворення типу заміна байтів та зсув рядків можна представити у вигляді підстановки.

– Знайти, на який елемент - байт в результаті перетворень буде змінено a_{ij} байт, якщо $a_{ij} = 89 + 3 \cdot i + 1$, i — номер реєстрації.

Завдання № 5 (6 балів). Служба технічної розвідки перехопила випромінювання шифруючого засобу та визначила $2 \cdot m$ бітів двійкової гами зашифрування, зробивши при цьому одну помилку. Визначте по $2 \cdot m$ символам закон формування гами зашифрування та сформуйте наступні $2 \cdot m$ символів, якщо $2 \cdot m$ перехоплених з помилкою символів наведені.

Примітка. Проаналізувати $2 \cdot m$ символів, зробити виправлення помилки, скласти та розв'язати систему лінійних рівнянь m - го порядку. Номер варіанту $R = i \pmod 8 + 1$, i — номер реєстрації.

Завдання № 6 (6 балів). У системі захисту інформації використовується направлене шифрування в групах точок еліптичної кривої (ЕК). Порядок базової точки G дорівнює $n_i = 2^{256+i \cdot 32}$, де i — номер реєстрації. Визначте необхідну довжину модуля RSA направленого шифрування при якій забезпечувалася б така ж стійкість, як і в групах точок ЕК, якщо потужність криптоаналітичної системи складає 10^9 операцій додавання на ЕС, що становить 0,1% від потужності RSA криптоаналітичної системи.

Завдання № 7 (6 балів). У виданому конкурсанту алгоритмі вірусу є дефект. Визначити в чому його суть та як його виправити.

Нижче наведені приклади варіантів завдань для програмної реалізації (від 1 до 12 балів в залежності від рівня та якості реалізації).

— Для усіх поліномів ступеню $m < 8$ програмно побудувати таблицю відповідних зворотних поліномів $h(x) = (g(x))^{-1} \bmod f(x)$ по заданому модулю $f(x)$ (наприклад, $f(x) = x^8 + x^4 + x^3 + x + 1$), використовуючи відповідні математичні методи.

— Для заданого модулю $f(x)$ (наприклад, $f(x)=x^8+x^4+x^3+x+1$, $m=8$) програмно знайти усі первісні елементи $g(x)$ поля $F(2^m)$, використовуючи необхідні та достатні умови первісності.

— Використовуючи заданий первісний елемент $g(x)$ (наприклад, $g(x)=x^4+1$) програмно побудувати усі елементи поля $F(2^m)$ при заданому модулю $f(x)$ (наприклад, $f(x)=x^8+x^4+x^3+x+1$, $m=8$).

2. Результати олімпіади та аналіз рівня підготовки конкурсантів

Всього в олімпіаді прийняла участь 31 особа із 10 вузів України (КПІ, ДнНУ, ХПУ, УАБС, СДУ, ХІВПС, ВДУ, ХНУРЕ, Національна юридична академія, НГУ). За результатами олімпіади місця розподілилися таким чином.

З напрямку "Інформаційна безпека" (командний залік):
1 місце – команда ХНУРЕ в складі: Балагура Д.С., Лавриненко С.С., Пінчук М.В. (каф. БІТ);
2 місце – команда НТУ "КПІ" в складі: Руденко О.В., Коваль А.О., Афонін О.О. (каф. ММЗІ);
3 місце – команда НГУ в складі: Калініченко В.П., Іванько А.М.;
4 місце – команда ХІВПС в складі: Сухов В.В., Бойко М.М., Єфіменко Я.В.

З напрямку "Інформаційна безпека" (особистий залік):
1 місце – Балагура Дмитро Сергійович (ХНУРЕ) – 52 бали;
2 місце – Руденко Олексій Володимирович (НТУ "КПІ") – 48 балів;
2 місце – Коваль Андрій Олегович (НТУ "КПІ") – 48 балів;
2 місце – Лавриненко Станіслав Сергійович (ХНУРЕ) – 48 балів.

З дисципліни "Захист інформації" (особистий залік):
1 місце – Вітріщенко Вікторія Анатоліївна (ХНУРЕ) – 29 балів;
2 місце – Перепияка Олена Миколаївна (УАБС, харківська філія) – 28 балів;
3 місце – Горбунов Олексій Вікторович (ХНУРЕ) – 24 бали;
3 місце – Серьга Михайло Олександрович (ДнНУ, ФТІ) – 24 бали.

З дисципліни "Програмне забезпечення захисту інформації":
1 місце – Афонін Олександр Олександрович (НТУ "КПІ") – 14 балів;
2 місце – Колибельников Олександр Іванович (ХНУРЕ) – 12 балів;
3 місце – Ілібман Володимир Григорович (НТУ "КПІ") – 12 балів.

За представленням особистих програмних засобів захисту інформації:
1 місце – Горбенко Юрій Іванович, Вервейко Віталій Миколайович за роботу "Система захисту інформації в корпоративній мережі" (ХНУРЕ);
2 місце - Єфіменко Ярослав Валерійович за роботу "Структура програмного забезпечення спеціалізованої АСУ" (ХІВПС);
3 місце – Іванько Артем Миколайович за роботу "Програмно – апаратний комплекс виявлення закладних пристроїв" (НГУ).

Крім того, за оригінальність розв'язку задач були нагороджені наступні учасники олімпіади: Горбунов О.В., Пінчук М.В., Рогова Л.С. (ХНУРЕ), Коваль А.О., Руденко О.В. (НТУ "КПІ"), Єфименко Я.В. (ХІВПС).

До основних недоліків у підготовці конкурсантів слід віднести наступне.

— При вивченні тем, наприклад цифрових підписів, студенти поверхово засвоюють алгоритми, не володіють уміннями доводити коректність алгоритмів цифрового підпису.

— Не всі студенти знають критерії та показники, що можуть бути застосовані при порівнянні різних алгоритмів цифрового підпису (наприклад в полях та групах точок еліптичних кривих).

— Студенти, що навчаються за іншими спеціальностями, не знають перспективні алгоритми криптозахисту (наприклад, алгоритм 21 століття RIJNDAEL, який затверджено в 2001 р. в США в якості державного стандарту).

— Недостатня, а то й слабка підготовки студентів з питань таких спеціальних розділів математики як теорія чисел, теорія груп взагалі та теорія еліптичних груп частково.
— Значна кількість студентів не може розробити модель розвідки та криптоаналізу, з помилками розв'язують системи рівнянь над полями GF(2).
— Деякі студенти не знають навіть проблемних питань випромінювання ПЕОМ взагалі та монітору частково.

Проведена олімпіада продемонструвала зросший рівень підготовленості магістрів та студентів з проблемних питань захисту інформації в напрямку "Інформаційна безпека", конкурсанти продемонстрували розуміння основних протиріч та орієнтацію 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 здатні вільно складати програми для вирішення складних криптологічних задач з використанням ПЕОМ.

В номінації "Захист інформації в системах та мережах", в якій виступали студенти інших спеціальностей (спеціальностей, що вивчали лише одну або дві загально освітні дисципліни з захисту інформації) студенти також показали зрослий рівень знань та умінь. Вони продемонстрували ознайомленість з проблемними питаннями та новітніми алгоритмами криптографічного захисту інформації. Але, на наш погляд, математичний рівень підготовки цих студентів у криптології недостатній.

В цілому слід відмітити суттєво зросший рівень знань, обізнаність студентів та магістрів з проблемними питаннями інформаційної безпеки, а також велику зацікавленість у вивченні сучасних методів та засобів захисту інформації.

Харьковский национальный университет радиоэлектроники

Поступила в редколлегию 15.04.2002