Лекція № 10 (НЕ 2.2, 2 год.). Асиметричні криптосистеми.

План лекції:

1. Асиметрична система RSA.
2. Асиметрична система Ель-Гамаля.

Зміст лекції:

1. Асиметрична система RSA.

Отже для обміну інформацією, зашифрованою за допомогою криптосистеми RSA, необхідно виконати такі кроки.

Крок 1. *Підготовчі обчислення*. Отримувач генерує два великих простих числа p і q (мінімум 128-бітних). Для нашого прикладу візьмемо p=7, q=11. Обчислимо добуток, ***модуль*** криптосистеми, $n=p\times q = 77$. Далі необхідно обчислити функцію Ейлера для цього модуля. Ми знаємо, що для простих чисел $\varphi(n)=(p-1)(q-1)$. Отже $\varphi(77)= 6\times10=60$. Тепер необхідно згенерувати ціле число, взаємно просте як з n, так і з $\varphi(n)$, наприклад, e=13.

Пара чисел (e,n) буде служити ***публічним ключем*** криптосистеми. У нашому випадку це буде пара (13, 77).

Тепер необхідно обчислити ***приватний ключ*** d, парний до обраного публічного. Для цього треба розв‘язати рівняння: $(d\times e) \bmod \varphi(n) = 1$. У відповідності з обчисленням мультиплікативного оберненого, будемо мати: $d= (1+k\times \varphi(n))/e$. Для k=8 отримуємо d=37. Отже приватним ключем буде служити пара чисел (d,n) – (37,77).

Крок 2. *Розповсюдження ключів*. Для шифрування інформації використовують публічний ключ (хоча можна використовувати і приватний). Для використання його розміщують на ресурсі, до якого мають доступ усі учасники інформаційного обміну. Зауважимо, що одним публічним ключем можуть користуватися усі, хто бажає обмінюватися з отримувачем зашифрованою інформацією. На відміну від симетричних криптосистем, тут немає необхідності для кожної пари учасників генерувати окрему пару ключів, адже розшифрувати інформацію за допомогою публічного ключа неможливо (в усякому разі, обчислювально складно). Таким чином, конфіденційність обміну інформації гарантується самим принципом обробки інформації. Єдине, що необхідно зробити, це захистити публічний ключ від підміни (про атаки на асиметричні криптосистеми дивись далі). Найпростіше, що можна зробити, це захистити каталог, де знаходяться ключі, від запису, однак найнадійнішим способом вважається сертифікація публічних ключів. Кожен, хто бажає захистити свій публічний ключ від підміни, повинен отримати сертифікат довірчого центру інфраструктури відкритих ключів, який прив‘язує ключ до його власника.

Приватний ключ не розповсюджується. Він використовується для розшифрування інформації та створення ***електронного цифрового підпису***, і повинен бути відомим лише його власникові.

На цьому підготовчі операції закінчено, і можна починати обмін захищеною інформацією.

Крок 3. *Шифрування інформації*. Криптосистемою RSA можна зашифрувати числа (коди літер) у діапазоні від 0 до n. Відправник повідомлення, використовуючи публічний ключ (e,n), у нашому випадку – (13,77), за допомогою формули $C_i=(M_i)^e \bmod n$ зашифровує своє повідомлення, де M_i – числове представлення чергової літери повідомлення, C_i – черговий символ криптограми. Наприклад, слово «БАНК» (яке має числове представлення «02 01 17 14» за таблицею заміни українського алфавіту. Яка починається з 01) зашифрується наступним чином:

$C_1= 2^{13} \bmod 77 = 30$;

$C_2 = 1^{13} \bmod 77 = 1$;

$C_3=17^{13} \bmod 77 =73$;

$C_4=14^{13} \bmod 77 = 49$.

Отже криптограма буде мати вигляд: «30 01 73 49». Очевидно, що шифр в нашому прикладі є шифром простої заміни. Як бачимо, літера «А», яка має код «01», не змінилася. Таку ж властивість мають «0» та n-1. Отже, не всі числа доцільно вибирати в якості кодів літер. Вважається правильним надавати для шифрування числа з діапазону [2, n-2]. Це дещо ускладнює розкриття шифру.

Зашифрований текст пересилається отримувачу відкритими каналами зв‘язку.

З наведеного способу шифрування може скластися враження, що піднесення великого цілого числа у великий степінь та взяття залишку за модулем третього великого числа є надзвичайно складною математичною задачею. Однак насправді це зовсім не так. Для ілюстрації цього наведемо алгоритм обчислення виразу $432^{678} \bmod 987$ [Гундарь].

Число 678 можна представити так: 678=512+128+32+4+2. Тоді $432^{678} \bmod 987=(432^{512}\times432^{128}\times432^{32}\times432^{4}\times432^{2}) \bmod 987$. Використовуючи основні властивості, наведені вище, можемо записати: $432^{678} \bmod 987=((432^{2} \bmod 987)\times(432^{4} \bmod 987)\times(432^{32} \bmod 987)\times(432^{128} \bmod 987) \times (432^{512} \bmod 987)) \bmod 987$.

Тепер обчислимо ступені числа 432:

$432^{2} \bmod 987 = 81$;

$432^{4} \bmod 987 =81^{2} \bmod 987 = 639$;

$432^{8} \bmod 987 = 639^{2} \bmod 987=690$;

$432^{16} \bmod 987= 690^{2} \bmod 987=366$;

$432^{32} \bmod 987=366^{2} \bmod 987=711$;

$432^{64} \bmod 987=711^{2} \bmod 987=177$;

$432^{128} \bmod 987=177^{2} \bmod 987=732$;

$432^{256} \bmod 987=732^{2} \bmod 987=870$;

$432^{512} \bmod 987=870^{2} \bmod 987=858$.

Підставляючи у наш вираз ці значення, отримаємо: $(81\times639\times711\times732\times858) \bmod 987= 204$.

Крок 4. *Розшифрування інформації*. Отримувач розшифровує зашифроване повідомлення «30 01 73 49», використавши тільки йому відомий приватний ключ (d,n) та формулу $M_i=(C_i)^d \bmod n$. Доведемо принципову можливість розшифрування зашифрованої на публічному ключі інформації: $(C)^d \bmod n = (M^e \bmod n)^d \bmod n = (M^e)^d \bmod n = (M^{ed}) \bmod n = (M^{1+k\varphi(n)}) \bmod n = M(M^{\varphi(n)}) \bmod n = M$. Таким чином, операція зашифрування на публічному та розшифрування на приватному ключі – взаємно зворотні.

У нашому випадку приватним ключем служить пара (37,77). Тоді отримаємо:

$M_1=30^{37} \bmod 77 = 2$;

$M_2=1^{37} \bmod 77 = 1$;

$M_3=73^{37} \bmod 77 =17$;

$M_4=49^{37} \bmod 77 =14$.

Маючи таблицю заміни, за кодами літер отримаємо «БАНК». Отже, ми вияснили методи зашифрування та розшифрування інформації у криптосистемі RSA. Залишилося вияснити один цікавий факт, характерний для цієї криптосистеми.

Спробуємо використати для зашифрування приватний ключ. Нехай повідомлення для зашифрування те ж саме: «БАНК» або «02 01 17 14». Зашифруємо її на приватному ключі (37,77). Отримаємо таке:

$C_1= 2^{37} \bmod 77 = 51$;

$C_2 = 1^{37} \bmod 77 = 1$;

$C_3=17^{37} \bmod 77 =52$;

$C_4=14^{13} \bmod 77 = 42$.

Тепер розшифруємо зашифроване повідомлення «51 01 52 42» на публічному ключі (13,77):

$M_1=51^{13} \bmod 77 = 2$;

$M_2=1^{13} \bmod 77 = 1$;

$M_3=52^{13} \bmod 77 =17$;

$M_4=42^{13} \bmod 77 = 14$.

Як бачимо, ми отримали відкрите повідомлення «БАНК» і таким методом. Отже криптосистема RSA симетрична відносно застосування парних ключів: можна зашифровувати інформацію на публічному ключі та розшифровувати на приватному і навпаки, зашифровувати на приватному, а розшифровувати – на парному до нього публічному ключі.

Чим цікава така особливість? Оскільки приватний ключ знає лише його власник, то отримувач зашифрованої на приватному ключі інформації, може бути впевненим у тому, що її отримано саме від власника приватного ключа, і він згоден з цією інформацією. Отже ми маємо ***аналог підписаного автором документа***. До цієї проблеми ми повернемось у наступних розділах.

Криптостійкість RSA.

Припустимо, що інформацію, яку перехопив зловмисник, зашифровано на публічному ключі (13,77). Якою інформацією володіє в такому разі зловмисник? По-перше, він має криптограму «30 01 73 49»; по-друге, має публічний ключ (13,77). Які зусилля треба йому прикласти для обчислення відкритого тексту? Як вже згадувалося, задача розшифрування для RSA еквівалентна задачі розкладання великого числа (а у нашому випадку – малого числа 77) на прості множники. У монографії [Б.Шнайєр] виконано розрахунок MIPS років (1 MIPS рік = 1 млн. інструкцій за секунду на протязі 1 року = $3{,}1\times10^{13}$ інструкцій), необхідних для розкладання великих чисел на прості множники. Ці дані можна побачити у таблиці.

Кількість розрядів n	Значення функції $L(n)$	Кількість MIPS років
512	$6{,}7\times10^{19}$	$2{,}1\times10^{6}$
576	$1{,}7\times10^{21}$	$5{,}5\times10^{7}$
960	$3{,}7\times10^{28}$	$1{,}2\times10^{15}$
1024	$4{,}4\times10^{29}$	$1{,}4\times10^{16}$

Тут в якості функції $L(n)$, яка задає апроксимацію швидкості найкращого на сьогодні алгоритму розкладання чисел на прості множники, метода решета числового поля, взято:

$$L(n) = \exp(1+\varepsilon)\sqrt{(\ln n)(\ln\ln n)^2}\ ,$$

де n – кількість двійкових розрядів у числі; ε – мала величина.

У кінці 1995 року лише єдиний раз вдалося практично реалізувати розкриття шифру RSA для 500-бітного ключа. Для цього за допомогою Інтернет були задіяні 1600 комп‘ютерів на протязі 5 місяців неперервної роботи. Тому автори RSA рекомендують використовувати таку довжину модуля n [Б.Шнайєр]:

- 768 біт – для приватних осіб;
- 1024 біти – для комерційної інформації;
- 2048 біт – для особливо таємної інформації.

Наведемо також таблицю порівняння криптостійкості симетричних та асиметричних криптосистем. У таблиці вказано, за яких довжин ключів досягається приблизно однакова стійкість симетричних та асиметричних систем до методу суцільного перебору ключів (метод «грубої сили»).

Довжина ключа симетричної криптосистеми (біт)	Довжина відкритого ключа асиметричної криптосистеми (біт)
56	384
64	512
80	768

112	1792
128	2304

Як бачимо, для досягнення однакової стійкості асиметричні криптосистеми використовують значно довший ключ (від 7 до 18 разів). Зрозуміло, що такий довгий ключ значно зменшує швидкодію асиметричних алгоритмів.

І, нарешті, визначимо які типи інформації вимагають більшої крипостійкості, а, значить, і більшої довжини ключів [Б.Шнайєр]:

Тип інформації	**Час життя**	**Довжина ключа, біт**
Тактична військова інформація	хв./год.	56-64
Оголошення про нову продукцію, злиття компаній	дні/тижні	64
Довготривалі бізнес-плани	роки	64
Торговельні секрети (н-д, рецептура)	10-річчя	112
Секрети водневої бомби	>40 років	128
Особи шпигунів	>50 років	128
Дипломатичні конфлікти	>60 років	128
Дані перепису населення	>100 років	>128

З таблиці видно, що з огляду на терміни зберігання інформації різних типів таємності, довжини ключів асиметричних криптосистем у 2048 біт не виглядають занадто параноїдальними.

2. Криптосистема Ель-Гамаля.

Стійкість криптосистеми Ель-Гамаля, розробленої у 1985 році, ґрунтується на складності задачі дискретного логарифмування у скінченому полі.

Для встановлення зашифрованого інформаційного обміну необхідно виконати наступні кроки.

Крок 1. *Попередні обчислення*. За допомогою криптографічно стійкого генератора випадкових чисел генерують просте число n таке, що обчислення логарифму за mod n практично важко реалізувати.

Також випадково обирають числа g та a з діапазону $[1,n-1]$ та обчислюють $h=g^a \bmod n$.

Тепер ми маємо публічний ключ: (n, g, h) та приватний – (n, a).

Крок 2. *Шифрування інформації*. Зашифровують числа m від 0 до n. Для шифрування виконують наступне:

- Обирають випадкове число r, яке належить інтервалу $[1,n-1]$ та взаємно просте з $n-1$.
- Обчислюють пару чисел C_1 та C_2 за формулами: $C_1=g^r \bmod n$; $C_2=mh^r \bmod n$.

Пара чисел C_1 та C_2 утворює шифрограму для числа m.

Крок 3. *Розшифрування інформації*. Розшифрування виконується за формулою: $m=C_2(C_1^a)^{-1} \bmod n$. Доведемо це. Підставимо значення C_1 та C_2 сюди: $m=mh^r(g^a)^{-1} \bmod n$. Оскільки $h=g^a \bmod n$, то:

$$m=mh^r(g^a)^{-1} \bmod n= mh^r(h^r)^{-1} \bmod n = m.$$

Таким чином ми довели еквівалентність прямого та оберненого перетворення.

Розглянемо приклад. Нехай n=29, g=2, a=5. Обчислимо $h=2^5 \bmod 29 = 3$.

Таким чином, ***публічний ключ*** – (29,2,3), ***приватний ключ*** – (29,5).

Нехай повідомлення m=11. Оберемо r=8 та обчислимо $C_1=2^8 \bmod 29 = 24$ і $C_2=(11\times 3^8) \bmod 29=19$. Отже в результаті обчислень ми маємо криптограму C=(24,19).

Розшифруємо отриману криптограму: $D(C)=19\times(24^5)^{-1} \bmod 29 = 11 \equiv m$.

Криптостійкість системи Ель-Гамаля.

Як правило, використовують модуль n криптосистеми довжиною 1024 біти, g – порядку 160 біт.

Безпосередня атака на систему Ель-Гамаля, атака обчислення приватного ключа за публічним, потребує обчислення дискретного логарифму, що для таких великих чисел, n та g перетворюється у математичну задачу надзвичайної обчислювальної складності. Однак імовірна вразливість криптосистеми Ель-Гамаля полягає в тому, що саме повідомлення міститься лише у C_2. Тому теоретично можливою видається атака, коли помноживши C_2 на g^u ($u\neq 0$), ми отримаємо шифротекст для повідомлення $\acute{m}=mg^u$.