DOI: https://doi.org/10.33216/2222-3428-2019-17-6

УДК 003.26.09

Кардашук В.С., Мірошниченко І.І.

АСИМЕТРИЧНІ АЛГОРИТМИ ШИФРУВАННЯ В БОТНЕТ МЕРЕЖІ

Об'єктом дослідження є алгоритми шифрування, які використані для майбутнього аналізу їхньої роботи в ботнет мережі. У статті наводиться загальна інформація про ботнет мережі, їхню архітектуру. Приводяться варіанти їхнього використання, та обґрунтовується вибір однієї з архітектур. Приведено загальні відомості про асиметричні алгоритми шифрування даних. Коротко описано ідею створення асиметричних алгоритмів шифрування даних. Коротко описано схему шифрування даних за допомогою алгоритму з відкритим ключем. Приведено основні принципи побудови криптосистем з відкритим ключем. Наведено деякі варіанти використання криптосистем з відкритим ключем, їхні переваги та недоліки проти симетричних криптосистем. Наводиться коротка історія розвитку алгоритму та опис реалізації формування закритого та відкритого ключів, шифрування даних та дешифрування даних з точки зору виконуваних математичних операцій алгоритму RSA (Рональд Райвест (R. Rivest), Аді Шамір (A. Shamir) і Леонардо Едельмані (L. Adleman)). Сформульовані переваги алгоритму RSA, що роблять його одним з фаворитів. Наводиться коротка історія розвитку алгоритму та опис реалізації формування закритого та відкритого ключів, шифрування даних та дешифрування даних з точки зору виконуваних математичних операцій алгоритму Ель – Гамаля. Сформульовані переваги алгоритму Ель-Гамаля, що роблять його одним з фаворитів. Наводиться коротка історія розвитку алгоритму та опис реалізації формування закритого та відкритого ключів, шифрування даних та дешифрування даних з точки зору виконуваних математичних операцій алгоритму NTRUEncrypt (Nth-degree TRUncated polynomial ring). Сформульовані переваги алгоритму NTRUEncrypt, що роблять його одним з фаворитів. Наведено, рекомендовані розробником параметри для забезпечення високого рівня криптостійкості, асиметричного алгоритму шифрування даних NTRUEncrypt.

Ключові слова: *ботнет мережа, алгоритм шифрування з відкритим ключем, RSA, ElGamal, NTRUEncrypt.*

Актуальність дослідження. Ботнет являє собою додаток або декілька додатків для отримання віддаленого доступу або контролю пристрою, та отримання інформації про роботу користувача. На даний момент це велика проблема, бо більшу частину ботнетів досить складно виявити. В більшості випадків їх використовують для незаконних та наносять неймовірних збитків, але й можуть використовуватися для контролю дій у великих компаніях, для забезпечення безпеки даних в компанії.

Постановка проблеми. Ботнет мережі створюють загрозу через зараження сотень мільйонів комп'ютерів. Наразі близько 60 відсотків усіх комп'ютерів, підключених до мережі інтернет у світі, є зараженими ботами та контролюються зловмисниками. До того ж ботнет може заражати не тільки комп'ютери але й «Інтернет речей», тобто сучасну побутову техніку, телевізори, камери спостереження, будь що, що має підключення до всесвітньої мережі.

В більшості ботнетів, які збирають та відправляють інформацію на сервер використовується шифрування даних. Здебільшого використовуються симетричні алгоритми шифрування. Але також можуть використовуватись й асиметричні алгоритми шифрування даних, які набагато складніші, але й безпечніші с точки зору їх дешифрування при несанкціонованому доступі до даних.

На даний момент є досить мало інформації про те, як саме асиметричні алгоритми шифрування працюють у ботнет мережах. До кінця не зрозуміло у яких випадках доцільно використовувати асиметричні алгоритми шифрування, а у яких ні.

Аналіз останніх досліджень і публікацій. На даний момент досліджень роботи криптосистем з відкритим ключем в ботнет мережах, принаймні у відкритому доступі, немає.

Мета статті. Описання загальних відомостей про ботнет та дослідження алгоритмів шифрування з відкритим ключем, які будуть використані в роботі.

Викладення основного матеріалу. Ботнет – це деяка кількість пристроїв, з'єднаних через мережу інтернет, на кожному з яких працює один або більше ботів. Ботнет програми найчастіше використовуються для здійснення атаки типу «відмова у наданні послуг» (DDoS), збору інформації, спам розсилок та отримання віддаленого контролю над пристроєм. Ботнет - це логічна колекція підключених до Інтернету пристроїв, таких як комп'ютери, смартфони або пристрої IoT (Internet of Things), безпека яких порушена і контроль переданий третій стороні. Кожен такий скомпрометований пристрій, відомий як "бот", створюється, коли на пристрій проникає програмне забезпечення. Контролер ботнету може керувати діяльністю цих компрометованих комп'ютерів за допомогою каналів зв'язку, утворених мережевими протоколами на основі стандартів, такими як IRC та протокол передачі гіпертексту (HTTP).

Архітектура ботнету розвивалася з часом, намагаючись уникнути виявлення та зриву. Традиційно бот програми будуються як клієнти, які спілкуються через існуючі сервери. Це дозволяє особі, яка управляє ботнетом здійснювати весь контроль із віддаленого місця, що обтяжує їхній трафік. Багато останніх ботнетів зараз для

спілкування покладаються на існуючі однорангові мережі. Ці бот-програми P2P (peer-2-peer) виконують ті ж дії, що і модель клієнт-сервер, але для комунікації їм не потрібен центральний сервер.[5]

У структурі бот-системи «клієнт-сервер», створюється базова мережа, в якій один сервер виступає в ролі ботмастера. Ботмастер контролює передачу інформації від кожного клієнта для установки команд і управління над клієнтськими пристроями.

Зазвичай ці ботнети працюють через мережі Інтернет-ретрансляційних чатів, домени чи веб-сайти. Заражені клієнти отримують доступ до заздалегідь визначеного місця та чекають вхідних команд із сервера. Управляючий посилає команди на сервер, який передає їх клієнтам. Клієнти виконують команди та звітують про свої результати назад до сервера.

Модель «клієнт-сервер» працює з допомогою спеціального програмного забезпечення і дозволяє ботмастеру зберігати постійний контроль над зараженими пристроями. Ця модель має декілька недоліків: її можна легко виявити, і вона має лише одну контрольну точку. У цій моделі, якщо сервер знищений, ботнет гине.

Але є й такий варіант якщо, наприклад, у якості командного центра використовується інтернет сторінка, тоді лише потрібно мати резервну копію вихідного коду серверної програми. А у якості шляху передачі файлів можуть слугувати анонімні сервіси електронної пошти. В більшості випадків такі ботнет мережі використовються для кейлогінгу, крадіжки даних або отримання віддаленого контролю над пристроєм.[5]

Замість того, щоб спілкуватися з централізованим сервером, P2P (Peer-2-Peer) – боти виконують функцію як сервера розподілу команд, так і клієнта, який отримує команди. Це дозволяє уникнути будь-якої точки відмови, що є проблемою централізованих ботнет мереж. Для того, щоб знайти інші заражені машини, бот стримано досліджує випадкові IP-адреси, поки він не зв'яжеться з іншою зараженою машиною. Контактний бот відповідає з такою інформацією, як його версія програмного забезпечення та список відомих ботів. Якщо версія одного з ботів нижча за іншу, вони ініціюють передачу файлів для оновлення. Таким чином, кожен бот розширює свій список заражених машин та оновлює себе, періодично спілкуючись з усіма відомими ботами. Бонети з архітектурою P2P найчастіше використовуються для зловживання платою за клік, наприклад в Google Ads, спаму або для атака «розподілена відмова в обслуговуванні» (DDoS).[5]

Шифрування в ботнет мережах використовується здебільшого при крадіжці даних, тому для розробки ботнет мережі в якій буде проводитися аналіз роботи асиметричних криптосистем обрано архітектуру клієнт-сервер.

Асиметричні криптографічні системи — це ефективні для захисту даних системи, які також називають криптографічними системами з відкритим ключем. Ці системи використовують один ключ для шифрування інформації та інший для її дешифрування. Перший ключ - відкритий, і він може бути оприлюднений для всіх, хто може використовувати систему шифрування. Відкритий ключ неможливо розшифрувати. Для розшифрування інформації другий ключ – закритий, таємний, його не можливо визначити на основі ключа шифрування.[2]

Основний результат асиметричних криптосистем у тому, що вони дозволили незахищеним користувачам спочатку ділитися конфіденційними повідомленнями. Та убрали необхідність перевіряти секретний ключ відправника та адресанта.[2]

Проблема управління ключами була вирішена шифруванням за допомогою відкритих або асиметричних ключів, концепція, запропонована Уїтфілдом Діффі та Мартіном Хеллманом у 1975 році. Шифрування відкритого ключа - це асиметрична схема, в якій використовується пара ключів.:

- Відкритий (public key) – використовується для шифрування даних;
- Закритий (private key) - використовується розшифровування даних.

Користувач поширює лише власний пеблічний ключ. Однак приватний тримається в таємниці. Коли хтось надсилає одержувачу лише повідомлення для читання, зашифруйте повідомлення відкритим ключем одержувача. Потім будь-яким способом відправляє зашифроване повідомлення одержувачу. Спочатку потрібно розшифрувати. Це можливо лише за допомогою приватного ключа, який є лише в пункті призначення. Звідси, якщо хтось, хто не має закритого ключа, отримав зашифровані дані, він не зможе їх прочитати.[2]

Отримувач, отримавши дані, дешифрує їх за допомогою закритого ключа, який є тільки в нього.

Хоча, ключі математично пов'язані, отримати приватній ключ з відкритого дуже складно, в практичному плані це займає дуже багато часу, що робить ці витрати необгрунтованими.

Нехай K – простір ключів, а e та d – ключі шифрування й дешифрування відповідно. E_e – функція шифрування для довільного ключа $e \in K$, така що:

$$E_e(c) = c) \tag{1}$$

Тут $c \in C$, де C – простів шифротекстів, а $m \in M$, де M – простір повідомлень.

D_d – функція дешифрування, з допомогою якої можна знайти похідне повідомлення m, знаючи шифротекст c:

$$D_d(c) = m \tag{2}$$

$\{E_e : e \in K\}$ – набір шифрування, а $\{D_d : d \in K\}$ – відповідний набір для дешифрування. Кожна пара *(E, D)* має властивість: знаючи E_e, неможливо вирішити рівняння $E_e(m) = c$, тобто для даного довільного шифротексту

$c \in C$, неможливо знайти $m \in M$. Це означає, що по даному e неможливо визначити відповідний ключ розшифрування d. E_e являє собою односторонню функцію, а d – лазівкою.

Основні принципи побудови криптосистем з відкритим ключем:

1. Починаємо з складної задачі *P*. Теоретично вона повинна рішатися складно: має не бути алгоритму, який зміг би перебрати всі варіанти рішення задачі *P* за ефективний час, відносно розміру задачі.
2. Можна виділити легку подзадачу *P'* з *P*. Вона повинна вирішуватися за поліноміальний час.
3. «Перетасовуємо» *P'*, щоб отримати задачу *P''*, взагалі не схожу на початкову. Задача *P''* повинна принаймні виглядати як оригінальна складновирішувана задача *P*.
4. *P''* подається з описом, як її можна бути використана для зашифрування. Як з *P''* отримати *P'*, залишається у секреті як секретна лазівка.
5. Криптографічна система влаштована так, що алгоритми розшифрування для користувача й криптоаналітика суттєво різні. В той час коли другий вирішує задачу *P''*, перший використовує секретну лазівку й вирішує *P'* – задачу.[2]

Алгоритми шифрування з відкритим ключем можна використовувати як:

- Самостійний засіб захисту інформації, яку передають та зберігають;
- Інструменти розподілу ключів (зазвичай використовують алгоритми шифрування відкритих ключів для розподілу дрібних клавіш на об'єм та інші алгоритми для передачі великих потоків даних) ;
- Засіб аутентифікації користувачів;

Переваги асиметричних шифрів перед симетричними:

- Не потрібно попередньо передавати ключ по надійному каналу;
- Тільки одній стороні відомий ключ дешифрування, який треба тримати у секреті;
- У великих мережах кількість ключів в асиметричній криптосистемі значно менше, ніж у симетричній;
- Складність розшифрування тексту, зашифрованого алгоритмом асиметричного шифрування, без закритого ключа значно віща, за розшифрування тексту, зашифрованого симетричним шифром, без ключа.[2]

Недоліки алгоритму асиметричного шифрування в порівнянні з симетричним:

- В алгоритм складніше вносити зміни;
- Більші ключі;
- Шифрування – розшифрування даних проходить довше.[2]

Одним з найпоширеніших криптографічних алгоритмів асиметричного шифрування є алгоритм RSA, названий на честь першої літери розробника: Рональд Рівест, А. Шамір, Леонардо Едельман. Алгоритм RSA, винайдений між 1977 і 1978 роками, став першим алгоритмом відкритого ключа, який застосовувався як для шифрування даних, так і для цифрових підписів. У 1993 році метод RSA був прийнятий як стандарт. На сьогодні RSA є одним із багатьох стандартів, включаючи Міжнародну організацію зі стандартизації (ISO), Міжнародний банк міжбанківських фінансових комунікацій (SWIFT), ANSI X9.31, французький стандарт ETVAS 5 та австралійський AS2805. .6.5.3 тощо. [2]

Безпека RSA заснована на складності розкладання великих чисел на множники. Відкритий й закритий ключі являються функціями двох великих простих чисел. Передбачається, що відновлення відкритого тексту по шифротексту й відкритому ключу еквівалентно розкладу на множники двох великих чисел. [3]

Для генерації ключів використовуються два великих простих числа p і q й розраховується їхній добуток:

$$n = p \cdot q \tag{3}$$

Далі обирається ключ шифрування *e*, такий що *e* й *(p-1)(q-1)* є взаємо простими числами. Після чого використовується розширений алгоритм Евкліда для обчислення ключа дешифрування *d*:

$$d = e^{-1} \, mod \, ((p-1)(q-1)) \tag{4}$$

Числа *e* і *n* – відкритий ключ, а *e* і *d* – закритий.

Формула шифрування виглядає так:

$$c = \, m^e \, mod \, n \tag{5}$$

Де, *c* – шифротекст, а *m* – початковий текст.

Для розшифрування треба обчислити:

$$m = \, c^d \, mod \, n \tag{6}$$

Алгоритм RSA було обрано через те, що це один з небагатьох алгоритмів шифрування з відкритим ключем, який при дешифруванні дає однозначний результат, а не, наприклад, кортеж з чотирьох варіантів дешифрування, як в криптосистемі Рабіна, його розповсюдженість й відносну легкість у реалізації.

ElGamal – криптографічна система з відкритим ключем, заснована на труднощах обчислення дискретних логарифмів у кінцевих полях. Криптографічна система включає алгоритми шифрування та алгоритми цифрового

підпису. Система El-Gamal є основою для старого стандарту цифрового підпису у США (DSA) та Росії (ГОСТ Р 34.10-94). [2]

Цю схему запропонував у 1985 році Тачер Ель-Гамал. Ель-Гамал розробив один із варіантів алгоритму Діффі-Гелмана. Він доповнив систему Діффі-Геллмана та розробива два алгоритми, розроблені для шифрування та аутентифікації. Алгоритм El-Gamal не запатентований і не вимагає ліцензійних платежів, що робить його дешевшою альтернативою. Вважається, що цей алгоритм підпадає під патент Diffie-Gellman. [1]

Для генерації пари ключів спочатку обирається просте число p й два числа, g й x, обидва числа повинні бути менше ніж p. Потім обчислюється:

$$y = g^x \bmod p \tag{7}$$

Відкритий ключ – це числа p, g ,y, а закритий ключ – x.

Для шифрування повідомлення M спочатку обирається сессійний ключ – ціле число k таке, $1<k<p-1$. Після чого обчислюються числа:

$$a = g^k \bmod p \tag{8}$$

$$b = y^k M \bmod p \tag{9}$$

Пара чисел a і b є шифротекстом.

Не складно помітити, що довжина шифротексту в схемі Ель-Гамаля довша за повідомлення удвічі.

Знаючи приватний ключ x , повідомлення можна обчислити з шифротексту за формулою:

$$M = b(a^x)^{-1} \bmod p \tag{10}$$

Але для практичних обчислень більше підходить така формула:

$$M = b \cdot a^{(p-1-x)} \bmod p \tag{11}$$

Цей алгоритм було обрано через ті самі причини що й алгоритм RSA, та те що криптостійкість алгоритму засновано на іншій математичній операції.

Криптосистема на основі решітчастої критосистеми NTRUEncrypt була створена як альтернатива RSA та криптографічній системі на Еліптичних кривих (ECC). Надійний алгоритм ускладнює пошук найкоротшого мережевого вектора, що робить його більш стійким до квантових комп'ютерних атак. На відміну від конкурентів RSA, ECC та ElGamal, алгоритм використовує операції над кільцем усічених многочленів, щоб не перевищувати N-1.

Алгоритм NTRU є відносно новою криптосистемою. Перша версія була розроблена близько 1996 року трьома математиками: Хофсгаймом, Піфером та Сільверманом. У 1996 році ці математики та Девід Ліман заснували корпорацію NTRU Cryptosystems і запатентували криптографічну систему. [4]

Сторони A і B потребують відкритого та приватного ключа, щоб надіслати повідомлення. Сторона B знає як відкритий так і закритий ключ, а сторона A тільки відкритий ключ. Сторона B використовую закритий ключ для генерації відкритого. Сторона B вибирає два "малих" полінома f і g від R. "Малість" многочлена розуміється як мала в порівнянні з будь-яким поліномним модулем q. Розподілений модуль q, q набагато менший для малих поліномів. Малість поліномів визначається за допомогою чисел df і dg:[4]

– поліном f має df коефіцієнтів, що рівні 1, і $df–1$ коефіцієнтів, які рівні -1, інші рівні 0. Тоді кажуть , що $f \in A$;

– поліном g має dg коефіцієнтів, що рівні 1, і стільки же, що рівні -1, інші рівні 0. Тоді кажуть, що $g \in A$.

Поліноми вибираються саме таким чином через те, що f, можливо, буде мати зворотній, а g – однозначно ні.

Сторона B повинна зберігати ці поліноми у секреті. Далі сторона B рахує зворотні поліноми f_p і f_q , тобто такі, що:

$$f \cdot f_p \equiv 1 \ (mod\ p) \text{ й} \tag{12}$$

$$f \cdot f_q \equiv 1 \ (mod\ q) \tag{13}$$

Якщо f не має зворотного поліному, то сторона B має вибрати інший поліном f.

Приватний ключ – це пара p (f, f_p) , а відкритий ключ h обчислюється за формулою:

$$h = \left(pf_q \cdot g\right) mod\ q \tag{14}$$

Тепер, коли у сторони А є відкритий ключ, вона може відіслати зашифровані дані стороні В. Для цього потрібно представити дані у вигляді поліному m з коефіцієнтами по модулю p, обраними з діапазону $[-p/2;\ p/2]$. Іншими словами, m - "малий" поліномний модуль q. Далі сторона А повинна вибрати інший "малий" многочлен r, що визначається за допомогою числа *dr*. Поліном *r* має *dr* коефіцієнтів, що дорівнюють *1*, і стільки ж, рівних *-1*, інші дорівнюють *0*. У цьому випадку кажуть, що $r \in A$.[6]

Використовуючи ці многочлени, зашифровані дані отримуємо по формулі:

$$e = (r \cdot h + m)\ mod\ q \tag{15}$$

При цьому кожен, хто має доступ або може вирахувати поліном r , матиме змогу прочитати дані m.

Тепер, отримавши зашифровані дані *e*, сторона В може його розшифрувати, використовуючи свій приватний ключ. Спочатку треба отримати проміжний поліном: [6]

$$a = (f \cdot e)\ mod\ q \tag{16}$$

Якщо розписати шифротекст, то отримаємо наступний ланцюг:

$$a = (f \cdot e)\ mod\ q = \big(f \cdot (r \cdot h + m)\big)\ mod\ q = \Big(f \cdot \big(r \cdot pf_q\ \cdot g + m\big)\Big)\ mod\ q \tag{17}$$

і в результаті:

$$a = (pr\ \cdot g + f \cdot g)\ mod\ q \tag{18}$$

Коли сторона В вирахувала многочлен a по модулю q, потрібно обрати його коефіцієнти з діапазону $[-q/2; q/2]$ і далі обчислити поліном b, що отримуємо із многочлену a приведенням його до модулю p:

$$b = a\ mod\ p = (f\ \cdot m)\ mod\ p \tag{19}$$

Тепер, використовуючи другу частину приватного ключа й отриманий многочлен *b*, сторона В може розшифрувати дані:

$$c = \big(f_p \cdot b\big)\ mod\ p \tag{20}$$

Алгоритм NTRUEncrypt є дуже перспективним алгоритмом асиметричного шифрування. Він має достатню стійкість від злому за допомогою квантового комп'ютеру та більш велику швидкість операцій, аніж у інших алгоритмах асиметричного шифрування. [6]

Розробники асиметричного алгоритму шифрування даних NTRUEncrypt, для забезпечення високої стійкості алгоритму, пропонують використовувати тільки рекомендовані параметри, які наведено в таблиці 1:

Таблиця 1. Рекомендовані параметри[4]

Позначення	*N*	*q*	*p*	*df*	*dg*	*dr*	Стійкість
NTRU167:3	167	128	3	61	20	18	Достатній рівень
NTRU251:3	251	128	3	50	24	16	Стандартний рівень
NTRU503:3	503	256	3	216	72	55	Найвищій рівень
NTRU167:2	167	127	2	45	35	18	Достатній рівень
NTRU151:2	251	127	2	35	35	22	Стандартний рівень
NTRU503:2	503	253	2	155	100	65	Найвищій рівень

Висновок. Для аналізу роботи в ботнет мережі обрано криптографічні алгоритми з відкритим ключем RSA, ElGamal, NTRUEncrypt. Проведено аналіз цих алгоритмів. Виділено сильніші їх сторони. Основними критеріями їх вибору стало те що, по-перше, це одні з найрозповсюдженіших алгоритмів асиметричного шифрування, по-друге, всі вони базуються на різних математичних складностях для злому.

Література

1. Elgamal T. A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms.[Електронний ресурс] 4.07.1985/Режим доступу до ресурсу : https://caislab.kaist.ac.kr/lecture/2010/spring/cs548/basic/B02.pdf.
2. Alfred J. Menezes; Paul C. van Oorschot; Scott A. Vanstone (August 2001). Handbook of Applied Cryptography. [Електронний ресурс] Режим доступу до ресурсу: - http://cacr.uwaterloo.ca/hac.
3. Bruce Schneier. Applied Cryptography. 2nd edition. Protocols, algorithms and source codes in C./ Bruce Schneier, 2002 – R. 346-355.
4. NTRU Cryptography [Електронний ресурс] / Security Innovation. – Режим доступу до ресурсу: http://www.securityinnovation.com/products/encryptionlibraries/ntru-cryptography.html - 15.01.2012 р. – Загол. з екрану.
5. Ping Wang, Baber Aslam, Cliff C. Zou. Handbook of Information and Communication Security. Peer-to-Peer Botnets — M. Springer — С. 335—350.
6. О.В.Бочаров. Досліджнення алгоритму шифрування NTRU, 2012. [Електронний ресурс]. Режим доступу до ресурсу: - http://www.hups.mil.gov.ua/periodic-app/article/9829/soi_2012_5_20.pdf

References

1. Elgamal T. A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms.[Web resource] 4.07.1985/ Resource access mode: https://caislab.kaist.ac.kr/lecture/2010/spring/cs548/basic/B02.pdf.
2. Alfred J. Menezes; Paul C. van Oorschot; Scott A. Vanstone (August 2001). Handbook of Applied Cryptography. [Web resource] Resource access mode: - http://cacr.uwaterloo.ca/hac.
3. Bruce Schneier. Applied Cryptography. 2nd edition. Protocols, algorithms and source codes in C./ Bruce Schneier, 2002 – R. 346-355.
4. NTRU Cryptography [Web resource] / Security Innovation. – Resource access mode: www/ URL: http://www.securityinnovation.com/products/encryptionlibraries/ntru-cryptography.html - 15.01.2012 р. – Загол. з екрану.
5. Ping Wang, Baber Aslam, Cliff C. Zou. Handbook of Information and Communication Security. Peer-to-Peer Botnets — M. Springer — С. 335—350.
6. O.V.Bocharov. Research of encryption algorithm NTRU, 2012, [Web resource]. Resource access mode - http://www.hups.mil.gov.ua/periodic-app/article/9829/soi_2012_5_20.pdf

Объектом исследования являются алгоритмы шифрования, использованные для будущего анализа их работы в ботнет сети. В статье приводится общая информация о ботнет сети, их архитектуру. Приводятся варианты их использования, и обосновывается выбор одной из архитектур. Приведены общие сведения о асимметричные алгоритмы шифрования данных. Коротко описано идею создания асимметричных алгоритмов шифрования данных. Коротко описана схема шифрования данных с помощью алгоритма с открытым ключом. Приведены основные принципы построения криптосистем с открытым ключом. Приведены варианты использования криптосистем с открытым ключом, их преимущества и недостатки против симметричных криптосистем. Приводится краткая история развития алгоритма и описание реализации формирования закрытого и открытого ключей, шифрование данных и дешифрования данных с точки зрения выполняемых математических операций алгоритма RSA (Рональд Райвест (R. Rivest), Ади Шамир (A. Shamir) и Леонардо Эдельман (L. Adleman)). Сформулированы преимущества алгоритма RSA, что делают его одним из фаворитов. Приводится краткая история развития алгоритма и описание реализации формирования закрытого и открытого ключей, шифрование данных и дешифрования данных с точки зрения выполняемых математических операций алгоритма Эль - Гамаля. Сформулированы преимущества алгоритма Эль-Гамаля, что делают его одним из фаворитов. Приводится краткая история развития алгоритма и описание реализации формирования закрытого и открытого ключей, шифрование данных и дешифрования данных с точки зрения выполняемых математических операций алгоритма NTRUEncrypt (Nth-degree TRUncated polynomial ring). Сформулированы преимущества алгоритма NTRUEncrypt, что делают его одним из фаворитов. Показано, рекомендованные разработчиком параметры для обеспечения высокого уровня криптостойкости, асимметричного алгоритма шифрования данных NTRUEncrypt
.***Ключевые слова:*** *ботнет сеть, алгоритм шифрования с открытым ключом, RSA, ElGamal, NTRUEncrypt.*

The object of the study is the encryption algorithms used for future analysis of their work on the botnet network. The article provides general information about botnet networks and their architecture. Options for their use are given, and the choice of one of the architectures is justified. General information about asymmetric data encryption algorithms is provided. The idea of creating asymmetric data encryption algorithms is briefly described. The scheme for encrypting data using the public key algorithm is briefly described. The basic principles of construction of public-key cryptosystems are given. Some examples of using public key cryptosystems, their advantages and disadvantages against symmetric cryptosystems are given. A brief history of algorithm development and a

description of the implementation of the formation of private and public keys, data encryption and decryption of data in terms of mathematical operations of the algorithm RSA (Ronald Rivest (R. Rivest), Adi Shamir (A. Shamir) and Leonardo Edelmani (L. Adleman)). Formulated the benefits of the RSA algorithm, which make it one of the favorites. A brief history of the algorithm development and a description of the implementation of the formation of private and public keys, data encryption and decryption of data in terms of performed mathematical operations of the algorithm of El - Gamal. The advantages of the El-Gamal algorithm are formulated, which make it one of the favorites. A brief history of the algorithm development and a description of the implementation of the formation of private and public keys, data encryption and decryption of data in terms of the mathematical operations of the algorithm NTRUEncrypt (Nth-degree TRUncated polynomial ring). The advantages of the NTRUEncrypt algorithm are formulated, making it one of the favorites. The options recommended by the developer are provided to provide a high level of cryptocurrency, an asymmetric NTRUEncrypt data encryption algorithm.
Keywords: *botnet network, public key encryption algorithm, RSA, ElGamal, NTRUEncrypt.*

Кардашук В.С. – к.т.н., доцент кафедри «комп'ютерних наук та інженерії» Східноукраїнського національного університету ім. В. Даля, e-mail: kardashuk1@gmail.com
Мірошниченко І.І. – студент групи КІ-18дм, кафедри «комп'ютерних наук та інженерії» Східноукраїнського національного університету ім. В. Даля, e-mail: furis6864@gmail.com