АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ, ПОСТАНОВКА ЗАДАЧІ

1. Формування проблеми

Протягом багатьох століть людство використовувало криптографічні методи для захисту інформації при її передачі та зберіганні. Приблизно до кінця XIX ст. ці методи стали об'єктом математичного вивчення. До теперішнього часу криптографія містить безліч результатів (теорем, алгоритмів), як фундаментальних, так і прикладних. Заняття криптографією неможливо без серйозної математичної підготовки. Галузь математики, що вивчає захист інформації, традиційно називається криптології [cryptology] і підрозділяється на криптографію [cryptography], що займається розробкою нових методів і обгрунтуванням їх коректності, і криптоаналіз [cryptanalysis], завдання якого - інтенсивне вивчення існуючих методів, часто з метою реального розкриття секретів іншої сторони. Криптографія та криптоаналіз перебувають у тісній взаємодії один з одним і з практичними потребами і розвиваються паралельно закритими урядовими організаціями багатьох держав і міжнародним науковим співтовариством.

В даний час існують тисячі криптографічних систем, реалізованих як програмно, так і апаратно. Серед них можна виділити системи, сам криптографічний принцип роботи яких тримається в секреті, як, наприклад, мікросхема Clipper, пропонована урядом США в якості криптографічного стандарту для телекомунікацій, і системи, алгоритм яких відкритий, а секретної є тільки певна, як правило невелика, порція інформації, звана (секретним) ключем [(secret) key] - до них відноситься більшість систем, реалізованих програмно і призначених для широкого використання. Поява в середині нашого століття перших електронно-обчислювальних машин кардинально змінило ситуацію. З проникненням комп'ютерів у різні сфери життя виникла принципово нова галузь господарства - інформаційна індустрія. Обсяг циркулюючої в суспільстві інформації з тих пір стабільно зростає за експоненціальним законом - він приблизно подвоюється кожні п'ять років. Фактично, на порозі нового тисячоліття людство створило інформаційну цивілізацію, в якій від успішної роботи засобів обробки інформації залежить саме добробут і навіть виживання людства в його нинішній якості. Події, що сталися за цей період зміни можна охарактеризувати наступним чином:

• обсяги оброблюваної інформації зросли за півстоліття на кілька порядків;

• склалося таке положення речей, що доступ до певних даних дозволяє контролювати значні матеріальні та фінансові цінності; інформація набула вартість, яку в багатьох випадках навіть можна підрахувати;

• характер оброблюваних даних став надзвичайно різноманітним і більше не зводиться виключно текстовим даними;

• інформація повністю "знеособлені", тобто особливості її матеріального уявлення втратили своє значення - порівняйте лист минулого століття і сучасне послання по електронній пошті;

• характер інформаційних взаємодій надзвичайно ускладнився, і поряд з класичною задачею захисту переданих текстових повідомлень від несанкціонованого прочитання і спотворення виникли нові завдання сфери захисту інформації, що раніше стояли і які вирішувались у рамках використовуваних "паперових" технологій - наприклад, підпис під електронним документом і вручення електронного документа "під розписку" - мова про подібні "нових" задачах криптографії ще попереду;

• суб'єктами інформаційних процесів тепер є не тільки люди, а й створені ними автоматичні системи, які діють за закладеною в них програмі;

• обчислювальні "здібності" сучасних комп'ютерів підняли на абсолютно новий рівень як можливості з реалізації шифрів, раніше немислимих через свою високої складності, так і можливості аналітиків щодо їх злому.

• Перераховані вище зміни призвели до того, що дуже швидко після поширення комп'ютерів в діловій сфері практична криптографія зробила в своєму розвитку величезний стрибок, причому відразу за кількома напрямками:

• по-перше, були розроблені стійкі блокові шифри з секретним ключем, призначені для вирішення класичної задачі - забезпечення секретності і цілісності переданих або збережених даних, вони досі залишаються "робочою конячкою" криптографії, найбільш часто використовуваними засобами криптографічного захисту;

• по-друге, були створені методи вирішення нових, нетрадиційних завдань сфери захисту інформації, найбільш відомими з яких є завдання підпису цифрового документа і відкритого розподілу ключів.

Як бачимо, термін "криптографія" далеко пішов від свого первісного значення - "тайнопис", "таємний лист". Сьогодні ця дисципліна об'єднує методи захисту інформаційних взаємодій абсолютно різного характеру, що спираються на перетворення даних по секретних алгоритмам, включаючи алгоритми, які використовують секретні параметри.

Підіб'ємо підсумки:

• криптографія - це набір методів захисту інформаційних взаємодій від відхилень від їх нормального, штатного протікання, викликаних зловмисними діями різних суб'єктів, методів, які базуються на секретних алгоритмах перетворення інформації, включаючи алгоритми, які не є власне секретними, але використовують секретні параметри;

• історично першим завданням криптографії був захист переданих текстових повідомлень від несанкціонованого ознайомлення з їх змістом, що знайшло відображення в самій назві цієї дисципліни, цей захист базується на використанні "секретної мови", відомої тільки відправнику і одержувачу, всі методи шифрування є лише розвитком цієї філософської ідеї;

• з ускладненням інформаційних взаємодій в людському суспільстві виникли і продовжують виникати нові завдання по їх захисту, деякі з них були вирішені в рамках криптографії, що вимагало розвитку принципово нових підходів і методів.

1. Призначення продукту

Даний програмний продукт призначений для широкого кола користувачів, так як багатьом людям, по мірі того як вони обмінюються інформацією, необхідно, щоб ця інформація була доступна тільки певному колу людей. Це програма, за допомогою якої ви легко зможете зашифрувати дані, а потім відправити їх електронною поштою другу, колезі по роботі, знаючи при цьому, що ваша інформація надійно зашифрована і не потрапить в чужі руки.

1. Постанова задачі

Розглянувши існуючі алгоритми шифрування, ми зупинили вибір на алгоритмі шифрування на AES(Rijndael).

Advanced Encryption Standard (AES), також відомий під назвою Rijndael — симетричний алгоритм блочного шифрування (розмір блока 128 біт, ключ 128/192/256 біт), фіналіст конкурсу AES і прийнятий в якості американского стандарту шифрування урядом США. Вибір припав на AES з розрахуванням на широке використання і активний аналіз алгоритму, як це було із його попередником, DES. Державний інститут стандартів і технологій США опублікував попередню специфікацію AES 26 жовтня 2001 року, після п'ятилітньої підготовки. 26 травня 2002 року AES оголошено стандартом шифрування. Станом на 2006 рік AES є одним із найпоширеніших алгоритмів симетричного шифрування.

Програма повинна зчитувати файл для шифрування/дешифрування, шифрувати/дешифрувати його згідно ключу, що користувач обирає сам. Ключ повинен вводитися користувачем в текстове поле програми. Результатом виконання програми є файл із зашифрованими даними, які неможливо прочитати.

Програма повинна мати графічний інтерфейс зрозумілий звичайному користувачеві і містити довідку.

Основні функції, що буде реалізовано:

* розробка інтерфейсу користувача;
* розробка функції шифрування;
* зчитування/запис файлів.

1. Програмне забезпечення сервера (необхідний мінімум)

* серверна версія ОС Windows або Linux;
* веб-сервер (Apache, Nginx, тощо);
* СКБД (бажано MySQL Server, якщо звертати увагу на безкоштовне використання та простоту налаштування);
* PHP (для обробки скриптів написаних мовою php).