МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Відокремлений структурний підрозділ
«Класичний фаховий коледж
Сумського державного університету»»

І НАУКОВО-МЕТОДИЧНА КОНФЕРЕНЦІЯ ВИКЛАДАЧІВ, СПІВРОБІТНИКІВ І СТУДЕНТІВ

«Технологія, освіта, наука – 2024»

ТЕЗИ ДОПОВІДЕЙ

(Конотоп, 13 червня 2024 року)

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Сумський державний університет

Відокремлений структурний підрозділ

«Класичний фаховий коледж

Сумського державного університету»

І НАУКОВО-МЕТОДИЧНА КОНФЕРЕНЦІЯ ВИКЛАДАЧІВ, СПІВРОБІТНИКІВ І СТУДЕНТІВ

«ТЕХНОЛОГІЯ, ОСВІТА, НАУКА – 2024»

ТЕЗИ ДОПОВІДЕЙ

(Конотоп, 13 червня 2024 року)

Конотоп

2024

Метою дослідження є, перетворення тексту вихідної програми в послідовність ДНК, яка синтезується будь-яким із доступних методів і розташовується всередині живої клітини.

Таким чином, мова Cello допомагатиме вченим генерувати біологічні схеми, які будуть успішно працювати всередині живих організмів.

Перспективи розвитку цієї новітньої технології - це застосування мови для програмування клітин не тільки в медицині, а й, наприклад, в сільському господарстві - для обробки сільгоспкультур. Це дозволить «розумним» бактеріям, при необхідності, самостійно виробляти інсектициди - хімічні препарати для винищення шкідників.

Література

1. http://www.nanonewsnet.ru/news/2016/cello-yazyk-programmirovaniya-zhivoi-kletki.
2. http://www.cellocad.org.
3. http://science.sciencemag.org.
4. http://znaimo.com.ua.

МЕТОДИ ШИФРУВАННЯ ІНФОРМАЦІЇ

Печенко С.В., *викладач*
ВСП «Класичний фаховий коледж СумДУ»

Криптографія - тайнопис, спеціальна система зміни звичайного листа, яка використовується з метою зробити текст зрозумілим лише для обмеженого числа осіб, які знають цю систему. Історія криптографії - ровесниця історії людської мови. Більше того, спочатку писемність сама по собі була криптографічного системою, тому що в древніх суспільствах нею оволоділи тільки обрані. Священні книги Стародавнього Єгипту, Стародавньої Індії тому приклади.

Спочатку криптографія вивчала методи шифрування інформації - оборотного перетворення відкритого (вихідного) тексту на основі секретного алгоритму або ключа в шифрований текст (шифротекст). В якості основного критерію періодизації криптографії використовують технологічні характеристики методів шифрування.

Серед найрізноманітніших способів шифрування можна виділити наступні основні методи:

— Алгоритми заміни або підстановки - символи вихідного тексту замінюються на символи іншого (або того ж) алфавіту відповідно до заздалегідь визначеною схемою, яка і буде ключем даного шифру. Окремо цей метод в сучасних криптосистемах практично не використовується через надзвичайно низьку криптостійкість.

— Алгоритми перестановки - символи оригінального тексту міняються місцями за певним принципом, що є секретним ключем. Алгоритм перестановки сам по собі має низьку криптостійкість, але входить складовою частиною до багатьох сучасних криптосистем.

— Алгоритми гамування - символи вихідного тексту складаються з символами якоїсь випадкової послідовності.

— Алгоритми, засновані на складних математичних перетвореннях вихідного тексту за деякою формулою. Багато з них використовують невирішені математичні завдання.

— Комбіновані методи. Послідовне шифрування вихідного тексту за допомогою двох і більше методів.

Розглянемо алгоритми заміни або підстановки. Для підвищення стійкості шрифту використовують поліалфавітні підстановки, в яких для заміни символів вихідного тексту використовуються символи кількох алфавітів. Простою версією такого шифру є шифр Віжинера. Це досить стійкий криптографічний шифр для свого часу - не знаючи ключового слова, його було дуже важко зламати. На основі такого методу шифрування працювала шифрувальна машина «Енігма» (рис.1).

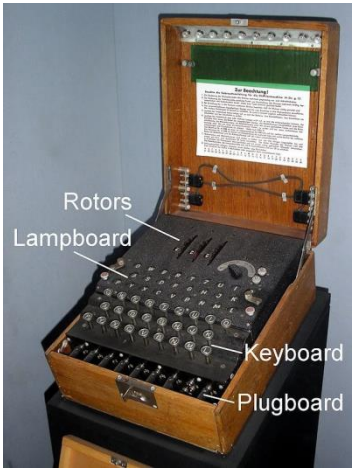

Рис. 1 Машина «Енігма»

Машина складалася з трьох роторів через які йшов струм, працювала шляхом постійної зміни електричного ланцюга за рахунок обертання внутрішніх роторів. При кожному натисненні букви на клавіатурі машина видавала букву шифру, а ротори ставали в нову позицію. Таким чином і працював поліалфавітний шифр підстановки..

Криптологічна бомба - апарат, вперше запропонований польським криптологом Маріаном Реєвським і розроблений в 1938 р. спільно з його колегами - математиками Єжимом Рожицьким і Генріхом Зигальським для систематичного розшифровування повідомлень. В часи Другої світової війни, на основі цієї розробки і при безпосередній підтримці її творців в Англії, був сконструйований найбільш «просунутий» агрегат. Головною метою Turing Bombe було знаходження налаштувань машини «Енігма», які потім використовували для розшифрування повідомлень з різних німецьких військових позицій.

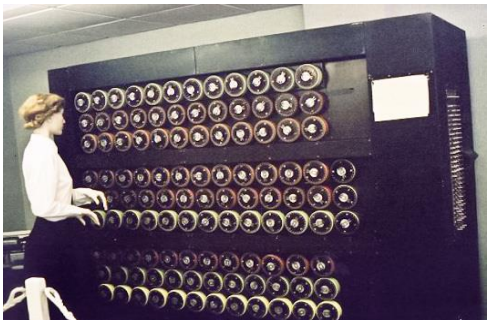

Рис. 2 Шифратор « Turing

Шифратор «Енігми» (рис2.) складався із 3-5 роторів з 26 електричними контактами. При натисненні кнопки на клавіатурі, електричний струм протікав через записуючий барабан на правому кінці скремблера, а потім через набір роторів у відбиваючий барабан, який повертав сигнал назад через ротори, і записуючий барабан. Під час роботи машини «Бомби» барабани, що знаходяться на верхньому ряду, обертаються із швидкістю 120 обертів за хвилину. Після того, як вони пройдуть повний оберт, середній ряд барабанів обертається на наступну позицію. Таким чином, методом перебору усі три ряди барабанів послідовно змінюють свій стан. Це триває до тих пір, поки положення роторів або приймає таке ж положення як при шифруванні, або барабани не повертаються у своє початкове положення. Питання лише полягало в тому, за яких умов відбувається такий збіг?

Теоретичну частину роботи виконав Алан Тьюринг. Принцип роботи розробленого Тьюрингом дешифратора полягав у переборі можливих варіантів ключа шифру і спроб розшифрування тексту, якщо була відома структура зашифрованого повідомлення або частина відкритого тексту.

В лютому 2015 року на екрани вийшов художній фільм «Гра в імітацію». Фільм був знятий за книгою Ендрю Ходжеса «Алан Тьюринг: Енігма». Він описує життя і роботу знаменитого англійського математика Алана Тьюрінга, який допоміг зламати код

німецької шифрувальної машини «Енігма» під час Другої світової війни. Хоча дія відбувається за часів Другої світової війни, але назва фільму відноситься до іншої наукової статті Алана Тьюринга, опублікованій в 1950 році під назвою «Обчислювальні машини й розум». В статті Тьюринг розглядає питання «Чи можуть машини думати?» і пропонує замінити термін «думати» на щось більш визначене.

Обґрунтований вибір тієї або іншої системи захисту загалом повинен спиратися на якісь критерії ефективності. На жаль, до цих пір не розроблені відповідні методики оцінки ефективності криптографічних систем. Найбільш простий критерій такої ефективності - вірогідність розкриття ключа або потужність безлічі ключів. По суті це те ж саме, що і криптостійкість. Для її чисельної оцінки можна використовувати також і складність розкриття шифру шляхом перебору всіх ключів. Проте, цей критерій не враховує інших важливих вимог до криптосистем:

— Неможливість розкриття або осмисленої модифікації інформації на основі аналізу її структури.

— Досконалість використовуваних протоколів захисту.

— Мінімальний об'єм використовуваної ключової інформації.

— Мінімальна складність реалізації (в кількості машинних операцій), її вартість.

— Висока оперативність.

Таким чином, сучасна криптографія утворює окремий науковий напрям на стику математики та інформатики. Практичне застосування криптографії стало невід'ємною частиною життя сучасного суспільства - її використовують в таких галузях як електронна комерція, електронний документообіг, телекомунікації та інших.

Література

1. В.В. Ященко: Введение в криптографию, М: МЦНМО, 2005р.-288с.
2. http://svitohlyad.com.ua/kompyutery.
3. http://ukr-article.com.
4. http://pidruchniki.com