КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ТАРАСА ШЕВЧЕНКА
Факультет комп’ютерних наук та кібернетики
Кафедра інтелектуальних програмних систем

Контрольна робота

з предмету «Математичні основи захисту інформації»

Варіант №5

Підготував:
Грищенко Юрій, ІПС-42

Київ – 2022

1. Частотна характеристика мови. Частотний метод криптоаналізу та методи боротьби з ним.

Важливе місце в характеристиці природної мови займає частота появи літер в її словах. Не всі літери алфавіту тієї, чи іншої природної мови появляються в словах з однаковою частотою. Одна літера появляється частіше за інші літери, а друга літера рідко появляється в тексті повідомлення.

Аналогічна ситуація має місце і для частоти появи двознаків, тризнаків і т. д.

Якщо текст зашифрований у відомому алфавіті, то частота появи символів в зашифрованому тексті несе певну інформацію про відкритий текст. Маючи в розпорядженні частоту появи символів алфавіту даної мови, криптоаналітик має можливість відтворити відкритий текст.

Короткий приклад частотного методу криптоаналізу: нехай зашифровано текст англійської мови.

Обчислюємо відносну частоту появи літер — для достатньо довгого тексту отримуємо розподіл, наближений до розподілу символів природної мови. Тоді зможемо зробити припущення, наприклад: літері, що зустрічається в шифрованому тексті найчастіше, відповідає літера E, а двознаку, що зустрічається найчастіше, скоріше за все відповідає “th”.

Карл Гаус запропонував метод боротьби: *гомофони* - відображенням однієї літери в декілька її образів. Кількість гомофонів для кожної літери повинна бути пропорціональна частоті появи цієї літери в явному тексті. Якщо гомофони використати ротаційно, то можна сподіватися, що частота появи літер не буде ідентична і це призведе до неможливості використання частотного криптоаналізу. Проте частота появи комбінацій сусідніх літер *дає можливість застосувати цей тип аналізу*.

Роторова машина Enigma, яка з кожним натисканням клавіші переходить на новий алфавіт підстановки, до того ж маючи більше 10000 алфавітів (з додаванням кожного ротора кількість збільшується в 26 разів), *знеможливлює частотний криптоаналіз*. На основі цього принципу створено багато сучасніших шифрів.

2. Довести, що бієктивна функція має обернену і що обернена функція теж буде бієкцією.

Доведемо, що коли $f : A \to B$ і $g : B \to A$ – довільні відображення, які задовольняють умову $f * g = \varepsilon_A$, то f – ін'єкція, а g – сюр'єкція. Дійсно, якщо $a, a' \in A$ і $f(a) = f(a')$, то $a = \varepsilon_A(a) = f * g(a) = g(f(a)) = g(f(a')) = f * g(a') = \varepsilon_A(a') = a'$. Отже, відображення f – ін'єкція. Якщо $a \in A$ – довільний елемент, то $a = \varepsilon_A(a) = f * g(a) = g(f(a))$, а це доводить сюр'єктивність відображення g.

Припустимо, що відображення f має обернене f^{-1}. Тоді із $f * f^{-1} = \varepsilon_A$ і $f^{-1} * f = \varepsilon_B$ випливає, що f сюр'єкція і ін'єкція, тобто f – бієкція.

Навпаки, припустимо, що f – бієкція. Тоді для довільного $b \in B$ знайдеться єдиний елемент $a \in A$, який є прообразом елемента b, тобто $f(a) = b$. Покладаючи $g(b) = a$, визначаємо відображення $g : B \to A$, яке задовольняє умові $f * g = \varepsilon_A$ і $g * f = \varepsilon_B$ Отже, $g = f^{-1}$.

Припустимо, що існує два відображення g і g', які обернені до відображення f, тобто $f * g = \varepsilon_A$ і $g * f = \varepsilon_B$ та $f * g' = \varepsilon_A$ і $g' * f = \varepsilon_B$. Тоді отримуємо $g' = \varepsilon_B * g' = (g * f) * g' = g * (f * g') = g * \varepsilon_A = g$.

Ми довели, що якщо f бієкція, то існує єдине f^{-1}. На тій же підставі відображення f^{-1} теж буде бієкцією. Із симетричності умов $f * f^{-1} = \varepsilon_A$ і $f^{-1} * f = \varepsilon_B$ випливає $(f^{-1})^{-1} = f$.

3. Абсолютно стійка криптосистема за Шенноном. Приклад такої системи.

Шеннон сформулював наступні припущення:

1. Криптоаналітику відомий тільки шифрований текст, тобто атака здійснюється на основі шифротексту.

2. Ключ і рандомізатор (засіб зрівнювання частотних характеристик тексту) використовуються для шифрування тільки один раз (тобто криптоаналіз здійснюється тільки по одній криптограмі).

3. На декартовому добутку задано ймовірнісний розподіл.

Позначимо m – повідомлення, c – криптограма. Тоді *абсолютно стійкою (цілком таємною)* криптосистемою S називається така криптосистема, для якої виконується одна з умов:

1. (∀(m,c)) p(m|c) = p(m); — відкритий текст і шифрований текст статистично незалежні.
2. H(m|c) = H(m); де H(m) і H(m|c) – ентропія і умовна ентропії відповідно; - відсутність в ШТ інформації відносно ВТ.

Для ключів k ∈ K та перетворення (шифрування) E_k сумісний розподіл ймовірностей криптограм і відкритих текстів на C x M індукується наступними співвідношеннями:

$$(\forall c,m)\, p(c,m) = p(m,c) = \sum_{\forall k, E_k(m)=c} p(m,k)$$

Тоді p(m|c) = p(m, c) / p(c).

Прикладом абсолютно стійкої криптосистеми є шифр Вернама, який використовується дотепер, і який покладено в основу сучасніших шифрів.

Обирається ключ такої самої довжини, як і довжина відкритого тексту. Ключ генерується як випадкова послідовність n незалежних рівноймовірних випадкових бітів з ймовірністю 2^{-n} незалежно від ВТ. Цей шифр краще всього служить для шифрування бінарних даних і описується таким чином:

$c_i = p_i$ XOR k_i

де

p_i – і-та бінарна цифра відкритого тексту

k_i – і-та бінарна цифра ключа

c_i – і-та бінарна цифра криптограми

Дешифрація ґрунтується на тій самій операції:

$p_i = c_i$ XOR k_i.

Головним недоліком шифру Вернама є велика довжина ключа, який потрібно попередньо передавати закритим каналом. В якості ключа береться “ідеальна” випадкова послідовність незалежних рівноймовірних випадкових бітів, тобто кожна реалізація довжини n з’являється з ймовірністю 2^{-n} незалежно від ВТ.

Якщо шифрується слово m, то ймовірність появи будь-якої ключової послідовності, а також будь-якої криптограми дорівнюватиме 2^{-n}.

$$p(c|m) = p(m)\frac{2^{-n}}{p(m)} = \frac{\sum_{(\forall k)E_k(m)=c} p(m,k)}{p(m)} = \frac{p(m)2^{-n}}{p(m)} = 2^{-n}$$

p(c) = p(c|m) = p(m,c)/p(m), звідси p(m|c) = p(m,c)/p(c) = p(m), отже система цілком таємна.

4. Означення одосторонньої функції з секретом. Основна властивість таких функцій.

Одностороння функція з секретом fk(x) = y називається функція, складність обчислення якої для всіх значень x належить до класу P, але обчислення $x = f^{-1}_k(y)$ майже для всіх значень y належить класу NP. Але, якщо скористатися секретною інформацією k, то для всіх значень y обчислення значення x такого, що $f_k(x) = y$ належить класу P.

В іноземній літературі такі функції називають функціями з “потайним ходом” (trapdoor function). Це поняття є основним в криптографії з відкритим ключем.

Гарантією існування односторонніх функцій служить гіпотеза, що P != NP. Оскільки ми не можемо строго довести існування односторонніх функцій, їх *основну властивість* можна описати так: ефективне обчислення значень функції нам відоме, тоді як жодні ефективні алгоритми обчислення значень обернених функцій невідомі.