

Математична криптологія

Афінні шифри



Шифр зсуву

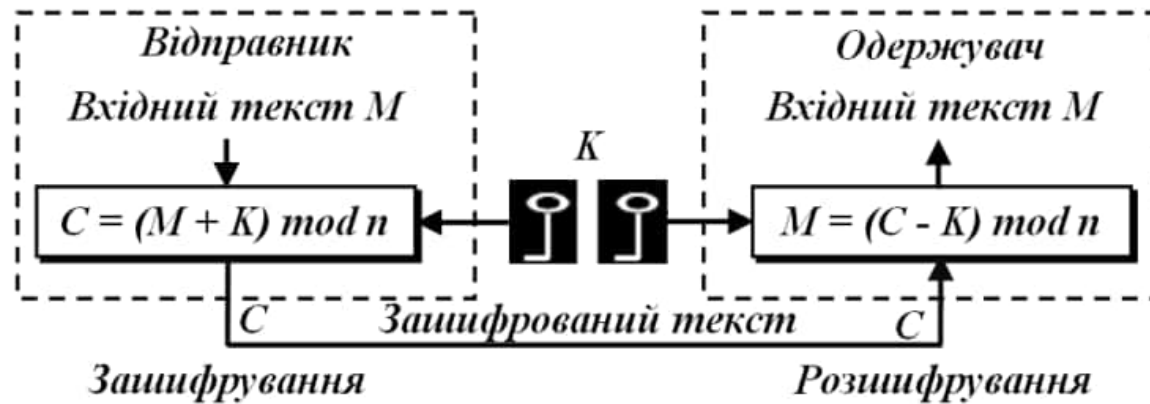
Афінні шифри - це підклас шифрів заміни, який включає як частковий випадок шифр Віженера та шифр перестановки з фіксованим періодом.

Шифр зсуву.

Ключ: s таке, що $0 \leq s < n$.

Шифрування. У повідомленні кожна буква x заміщується буквою $E(x) = (x + s) \bmod n$.

Дешифрування. У криптотексті кожна буква x' заміщується буквою $D(x') = (x' + s') \bmod n$, де $s' = n - s$. Величину зворотнього зсуву s' будемо називати *дешифруючим ключем*.



Шифр зсуву

Приклад: Зашифрувати повідомлення “hello” з використанням шифру зсуву з ключем $K = 15$.

Розв'язання:

$$m_1 = h \rightarrow 07; \quad c_1 = (07 + 15) \bmod 26 = 22 \rightarrow W;$$

$$m_2 = e \rightarrow 04; \quad c_2 = (04 + 15) \bmod 26 = 19 \rightarrow T;$$

$$m_3 = l \rightarrow 11; \quad c_3 = (11 + 15) \bmod 26 = 0 \rightarrow A;$$

$$m_4 = l \rightarrow 11; \quad c_4 = (11 + 15) \bmod 26 = 0 \rightarrow A;$$

$$m_5 = o \rightarrow 14; \quad c_5 = (14 + 15) \bmod 26 = 3 \rightarrow D;$$

як наслідок отримаємо зашифроване повідомлення “WTAAD”.

Приклад: Розшифрувати повідомлення “WTAAD”, використовуючи адитивний шифр з ключем $K = 15$.

Розв'язання: Застосовуємо алгоритм розшифрування (2.2) до зашифрованого тексту літера за літерою:

$$c_1 = W \rightarrow 22; \quad m_1 = (22 - 15) \bmod 26 = 07 \rightarrow h;$$

$$c_2 = T \rightarrow 19; \quad m_2 = (19 - 15) \bmod 26 = 04 \rightarrow e;$$

$$c_3 = A \rightarrow 00; \quad m_3 = (00 - 15) \bmod 26 = 11 \rightarrow l;$$

$$c_4 = A \rightarrow 00; \quad m_4 = (00 - 15) \bmod 26 = 11 \rightarrow l;$$

$$c_5 = D \rightarrow 03; \quad m_5 = (03 - 15) \bmod 26 = 14 \rightarrow o,$$

як наслідок отримаємо вихідне повідомлення “hello”.

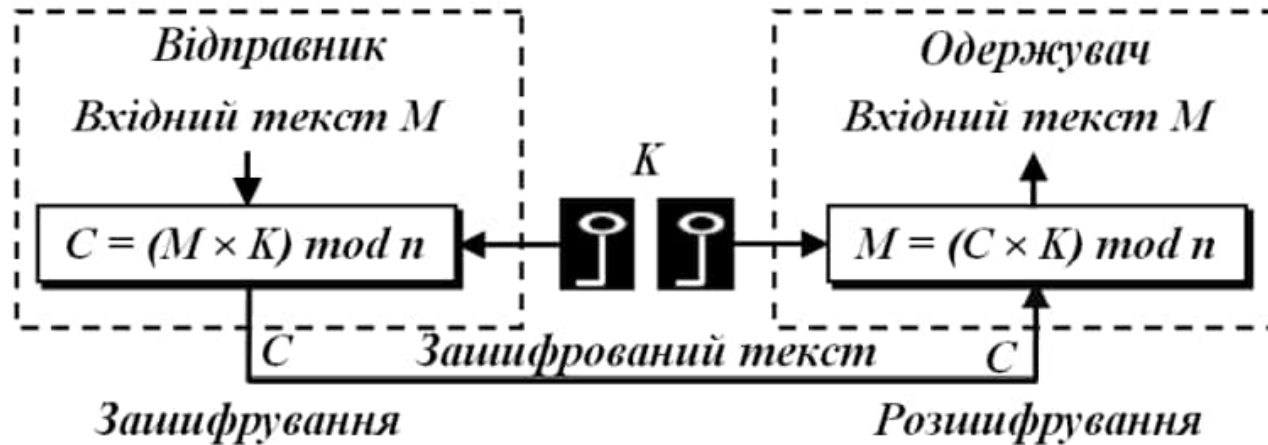
Лінійний шифр

ЛІНІЙНИЙ ШИФР.

Ключ: a таке, що $0 < a < n$ і $\text{НСД}(a, n) = 1$.

Шифрування. У повідомленні кожна буква x заміщується буквою $E(x) = (ax) \bmod n$.

Дешифрування. У криптотексті кожна буква x' заміщується буквою $D(x') = (a'x') \bmod n$, де $a' = a^{-1} \bmod n$ — дешифруючий ключ.



Лінійний шифр

Приклад 3.1. Припустимо, повідомлення записуються українською абеткою без пропусків між словами та розділових знаків, тобто $n = 33$. Нехай для шифрування використовується ключ $a = 2$. За допомогою розширеного алгоритму Евкліда знаходимо, що $a' = 17$ (див. приклад 2.9). Розглянемо процедуру шифрування повідомлення *завтра*. У цифровій формі воно представляється послідовністю чисел $9, 0, 2, 22, 20, 0$. Множення на 2 за модулем 33 дає послідовність $18, 0, 4, 11, 7, 0$, яка відповідає криптотекстові *oagiea*.

Співвідношення $D(E(x)) = x$ для будь-якого $x \in \mathbb{Z}_n$ доводиться просто: $a'(ax) = (a'a)x = 1x = x$ (операції виконуються в \mathbb{Z}_n). Існування a' для a гарантоване умовою $\text{НСД}(a, n) = 1$ за твердженням 2.8. Більше того, a' для заданого a ефективно обчислюється за допомогою розширеного алгоритму Евкліда (приклад 2.9). Нарешті покажемо, що ті a , які не задовольняють накладену нами умову, непридатні для використання в якості ключа.

ТВЕРДЖЕННЯ 3.2. *Відображення $E: \mathbb{Z}_n \rightarrow \mathbb{Z}_n$, задане формулою $E(x) = (ax) \bmod n$, має обернене тоді і тільки тоді, коли $\text{НСД}(a, n) = 1$.*

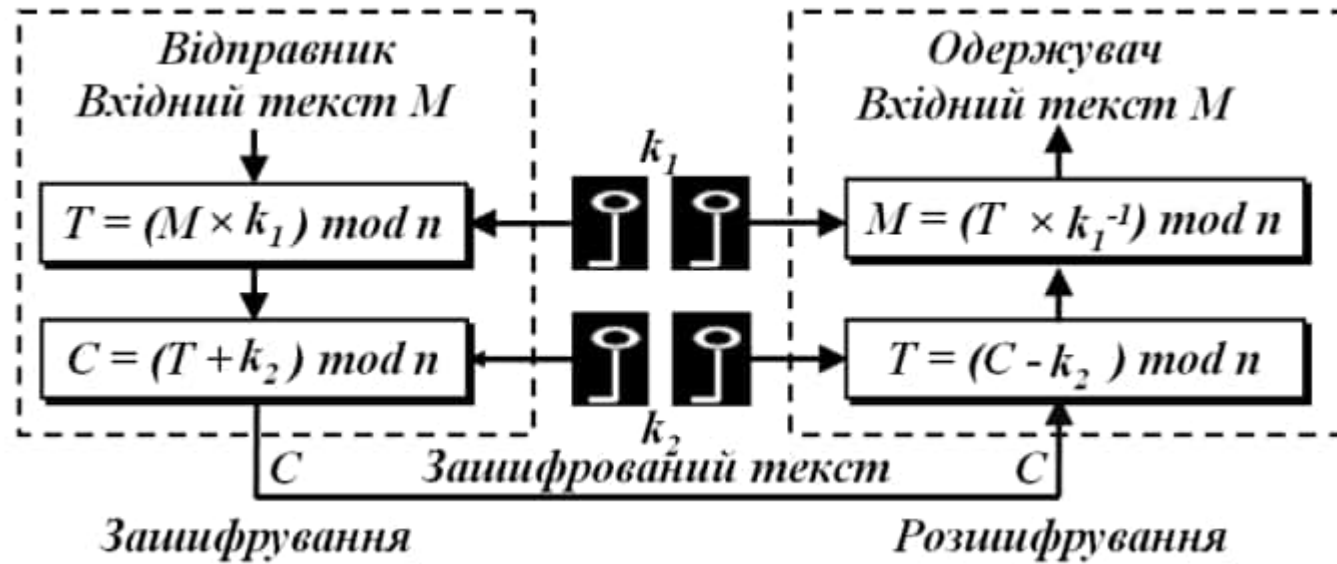
ДОВЕДЕННЯ. В один бік твердження нами щойно було доведено. Навпаки, припустимо, що відображення E має обернене. За теоремою про обернене відображення (див. кінець пункту 1.1), E сюр'єктивне. Позначимо через e прообраз одиниці: $E(e) = 1$. Це означає, що $ae \equiv 1 \pmod{n}$, звідки й випливає, що $\text{НСД}(a, n) = 1$. ■

Афінний шифр

Ключ: a, s такі, що $0 \leq s < n$, $0 < a < n$ і $\text{НСД}(a, n) = 1$.

Шифрування. У повідомленні кожна буква x заміщується буквою $E(x) = (ax + s) \bmod n$.

Дешифрування. У криптотексті кожна буква x' заміщується буквою $D(x') = (a'x' + s') \bmod n$, де пара $a' = a^{-1} \bmod n$ і $s' = (-a's) \bmod n$ є дешифруючим ключем.



Афінний шифр

Приклад. Використовуючи афінний шифр, зашифрувати повідомлення “hello” з ключовою парою $k_1 = 7$ і $k_2 = 2$.

$$m_1 = h \rightarrow 7; \quad c_1 = (7 \times 7 + 2) \bmod 26 = 25 \rightarrow Z;$$

$$m_2 = e \rightarrow 4; \quad c_2 = (4 \times 7 + 2) \bmod 26 = 4 \rightarrow E;$$

$$m_3 = l \rightarrow 11; \quad c_3 = (11 \times 7 + 2) \bmod 26 = 1 \rightarrow B;$$

$$m_4 = l \rightarrow 11; \quad c_4 = (11 \times 7 + 2) \bmod 26 = 1 \rightarrow B;$$

$$m_5 = o \rightarrow 14; \quad c_5 = (14 \times 7 + 2) \bmod 26 = 22 \rightarrow W: \text{отримаємо зашифроване повідомлення “ZEBBW”}.$$

Приклад. Використовуючи афінний шифр розшифрувати повідомлення “ZEBBW” із ключовою парою $k_1 = 7$ і $k_2 = 2$.

Розв’язування.

Щоб знайти символи вхідного тексту, додамо адитивну інверсію від $(-k_2) \bmod 26 = (-2) \bmod 26 = 24$ до отриманого зашифрованого тексту. Потім помножимо результат на мультиплікативну інверсію від

$$k_1^{-1} \bmod 26 = 7^{-1} \bmod 26 = 15.$$

$$c_1 = Z \rightarrow 25; \quad m_1 = ((25 + 24) \times 15) \bmod 26 = 7 \rightarrow h;$$

$$c_2 = E \rightarrow 4; \quad m_2 = ((4 + 24) \times 15) \bmod 26 = 4 \rightarrow e;$$

$$c_3 = B \rightarrow 1; \quad m_3 = ((1 + 24) \times 15) \bmod 26 = 11 \rightarrow l;$$

$$c_4 = B \rightarrow 1; \quad m_4 = ((1 + 24) \times 15) \bmod 26 = 11 \rightarrow l;$$

$$c_5 = W \rightarrow 22; \quad m_5 = ((22 + 24) \times 15) \bmod 26 = 14 \rightarrow o. \text{ Отже, отримаємо вихідне повідомлення “hello”}.$$

Афінний шифр

Вправа для самостійного виконання:

Довести, афінний шифр утворює групу. Знайти порядок цієї групи як функцію n . Обчислити його при $n = 26, 33$.



Шифр зсуву k -ого порядку (шифр Віженера з періодом k)

3.2. Афінні шифри вищих порядків. Подумаємо, як можна розширити монограмні шифри попереднього пункту так, щоб вони оперували з k -грамами для довільного $k > 1$. Спочатку введемо операцію додавання в \mathbb{Z}_n^k . Сумою векторів $X = (x_1, \dots, x_k)$ і $S = (s_1, \dots, s_k)$ з \mathbb{Z}_n^k є вектор $X + S = ((x_1 + s_1) \bmod n, \dots, (x_k + s_k) \bmod n)$. \mathbb{Z}_n^k з операцією додавання є групою. Вектор $-S = (n - s_1, \dots, n - s_k)$ є оберненим до вектора $S = (s_1, \dots, s_k)$.

Шифр зсуву k -го порядку (шифр Віженера з періодом k).

Ключ: $S \in \mathbb{Z}_n^k$.

Шифрування. Повідомлення розбивається на k -грами. Кожна k -грама X заміщується k -грамою $E(X) = X + S$.

Дешифрування. Кожна k -грама X' криптотексту заміщується k -грамою $D(X') = X' + S'$, де $S' = -S$ є дешифруючим ключем.

Лінійний шифр k -ого порядку

Перед тим як перейти до лінійного шифру нагадаємо, що через $M_k(\mathbb{Z}_n)$ ми позначаємо множину матриць розміру $k \times k$ з коефіцієнтами з кільця \mathbb{Z}_n , а через $GL_k(\mathbb{Z}_n)$ — підмножину оборотних матриць. Для $A \in GL_k(\mathbb{Z}_n)$ обернену до неї матрицю позначаємо через A^{-1} . Добутком AX матриці $A = (a_{ij})$ з $M_k(\mathbb{Z}_n)$ на вектор-стовпчик $X =$

(x_1, \dots, x_k) з \mathbb{Z}_n^k є вектор-стовпчик

$$\begin{pmatrix} a_{11} & a_{12} & a_{1k} \\ a_{21} & a_{22} & a_{2k} \\ a_{k1} & a_{k2} & a_{kk} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_k \end{pmatrix} = \begin{pmatrix} a_{11}x_1 + a_{12}x_2 + \dots + a_{1k}x_k \\ a_{21}x_1 + a_{22}x_2 + \dots + a_{2k}x_k \\ a_{k1}x_1 + a_{k2}x_2 + \dots + a_{kk}x_k \end{pmatrix}$$

Лінійний шифр k -го порядку.

Ключ: $A \in GL_k(\mathbb{Z}_n)$.

Шифрування. Повідомлення розбивається на k -грами. Кожна k -грама X заміщується k -грамою $E(X) = AX$.

Дешифрування. Кожна k -грама X' криптотексту заміщується k -грамою $D(X') = A'X'$, де $A' = A^{-1}$ — дешифруючий ключ.

Лінійний шифр k -ого порядку

Приклад 3.4. Лінійний шифр 1-го порядку обговорювався у попередньому пункті. Розглянемо докладніше випадок $k = 2$, тобто біграмний лінійний шифр. В якості ключа вибирається матриця $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ з коефіцієнтами $a, b, c, d \in \mathbb{Z}_n$. Матриця A повинна бути оборотною. За твердженням Б.5 це рівнозначно умові НСД(w, n) = 1 для $w = ad - bc$ — визначника матриці. За цієї умови з допомогою розширеного алгоритму Евкліда ми можемо знайти в \mathbb{Z}_n обернений елемент w^{-1} і за формулою оберненої матриці обчислити дешифруючий ключ

$$A' = \begin{pmatrix} dw^{-1} \bmod n & -bw^{-1} \bmod n \\ -cw^{-1} \bmod n & aw^{-1} \bmod n \end{pmatrix}$$

Наприклад, для $A = \begin{pmatrix} 1 & 1 \\ 32 & 1 \end{pmatrix}$ над \mathbb{Z}_{33} маємо $w = 2$. За розширеним алгоритмом Евкліда знаходимо $w^{-1} = 17$ (див. приклад 2.9) і

$$A' = \begin{pmatrix} 17 & 16 \\ 17 & 17 \end{pmatrix}$$

Лінійний шифр k -ого порядку

Нехай потрібно зашифрувати повідомлення завтра. Першій біграмі за відповідає вектор $\begin{pmatrix} 9 \\ 0 \end{pmatrix}$. Множення на матрицю A дає $\begin{pmatrix} (1 \cdot 9 + 1 \cdot 0) \bmod 33 \\ (32 \cdot 9 + 1 \cdot 0) \bmod 33 \end{pmatrix} = \begin{pmatrix} 9 \\ 24 \end{pmatrix}$. Таким же чином знаходимо образи біграм $вт = \begin{pmatrix} 2 \\ 22 \end{pmatrix}$ та $ра = \begin{pmatrix} 20 \\ 0 \end{pmatrix}$. Зауважимо, що множення матриці A на три вектори-біграми еквівалентне множенню цієї матриці на матрицю розміру 2 на 3:

$$\begin{pmatrix} 1 & 1 \\ 32 & 1 \end{pmatrix} \begin{pmatrix} 9 & 2 & 20 \\ 0 & 22 & 0 \end{pmatrix} = \begin{pmatrix} 9 & 24 & 20 \\ 24 & 20 & 13 \end{pmatrix}$$

Насамкінець перетворюємо стовпчики отриманої матриці у біграми і отримуємо криптотекст **зффррй**.

Дешифрування відбувається так само, лише із використанням оберненої матриці. Наприклад, якщо ми маємо криптотекст **рґк**, то розбиваємо його на біграми $\begin{pmatrix} р & г \\ ь & к \end{pmatrix} = \begin{pmatrix} 20 & 3 \\ 30 & 14 \end{pmatrix}$ і виконуємо множення на матрицю A' :

$$\begin{pmatrix} 17 & 16 \\ 17 & 17 \end{pmatrix} \begin{pmatrix} 20 & 3 \\ 30 & 14 \end{pmatrix} = \begin{pmatrix} 17 & 17 \\ 10 & 11 \end{pmatrix} = \begin{pmatrix} н & н \\ и & і \end{pmatrix}$$

В результаті дістаємо повідомлення **нині**.

Лінійний шифр k -ого порядку

Повернемось до загального аналізу лінійного шифру. Співвідношення $D(E(X)) = X$ для будь-якого $X \in \mathbb{Z}_n^k$ впливає з рівностей $A'(AX) = (A'A)X = I_k X = X$, де I_k — одинична матриця порядку k . Дешифруючий ключ A' для вибраної оборотною матриці A обчислюється ефективно за формулою для оберненої матриці (див. пункт Б.6). Потрібне для цього значення $(\det A)^{-1} \bmod n$ знаходиться за допомогою розширеного алгоритму Евкліда (приклад 2.9). На довершення доведемо, що необоротні матриці A непридатні для використання в якості ключа.

ТВЕРДЖЕННЯ 3.5. *Відображення $E: \mathbb{Z}_n^k \rightarrow \mathbb{Z}_n^k$, задане формулою $E(X) = AX$, має обернене тоді і тільки тоді, коли $A \in GL_k(\mathbb{Z}_n)$.*

Доведення. При $A \in GL_k(\mathbb{Z}_n)$ існування відображення, оберненого до E , було встановлене вище. Навпаки, припустимо, що E має обернене відображення D . Позначимо через X_i , $1 \leq i \leq k$, вектор з i -тою компонентою 1 і з рештою компонент, що дорівнюють 0. Розглянемо матрицю U із стовпчиками $D(X_1), \dots, D(X_k)$. Зауважимо, що $AU = I_k$, тобто матриця U є правою оберненою до A . Отже, матриця A оборотна (див. твердження Б.5). ■

Афінний шифр k -ого порядку

АФІННИЙ ШИФР k -ГО ПОРЯДКУ.

Ключ: $A \in GL_k(\mathbb{Z}_n)$ і $S \in \mathbb{Z}_n^k$.

Шифрування. Повідомлення розбивається на k -грами. Кожна k -грама X заміщується k -грамою $E(X) = AX + S$.¹

Дешифрування. Кожна k -грама X' криптотексту заміщується k -грамою $D(X') = A'X' + S'$, де $A' = A^{-1}$ і $S' = -A'S$ — дешифруючий ключ.

Приклад 3.6. Хочемо зашифрувати повідомлення **завтра** за допомогою ключа $A = \begin{pmatrix} 1 & 1 \\ 32 & 1 \end{pmatrix}$ і $S = \begin{pmatrix} 1 \\ 15 \end{pmatrix}$ над \mathbb{Z}_{33} .

Частина роботи вже виконана нами у прикладі 3.4. Після розбиття повідомлення на вектори-біграми і множення їх на матрицю A за модулем 33 ми були отримали $\begin{pmatrix} 9 & 24 & 20 \\ 24 & 20 & 13 \end{pmatrix}$. Додаємо до кожного стовпчика вектор S і отримуємо $\begin{pmatrix} 10 & 25 & 21 \\ 6 & 2 & 28 \end{pmatrix} = \begin{pmatrix} \mathbf{и} & \mathbf{х} & \mathbf{с} \\ \mathbf{е} & \mathbf{в} & \mathbf{ш} \end{pmatrix}$ тобто криптотекст **ихвсш**.

Знайдемо також дешифруючий ключ. У прикладі 3.4 була отримана матриця $A' = \begin{pmatrix} 17 & 16 \\ 17 & 17 \end{pmatrix}$. Обчислюємо $S' = -\begin{pmatrix} 17 & 16 \\ 17 & 17 \end{pmatrix} \begin{pmatrix} 1 \\ 15 \end{pmatrix} = \begin{pmatrix} 7 \\ 25 \end{pmatrix}$.

Криптоаналіз

3.3. Криптоаналіз. Атака з вибором відкритого тексту. Нескладно зауважити, що афінний шифр нестійкий до цього виду криптоаналізу. Позначимо через X_i , $1 \leq i \leq k$, вектор з i -тою компонентою 1 і з рештою компонент, що дорівнюють 0, а через X_0 нульовий вектор. Суперникові досить довідатись, в які криптотексти переходять відповідні цим векторам k -грами. Справді, $E(X_0) = S$, а образ $E(X_i)$ рівний i -тому стовпчику матриці A , що дозволяє повністю визначити ключ.

Атака з відомим відкритим текстом. Спочатку покажемо, що лінійний шифр вразливий від такої атаки. Припустимо суперник знає, що шифруєче відображення $E(X) = AX$ перетворює вектори X_1, \dots, X_k у вектори X'_1, \dots, X'_k . Сформуємо із стовпчиків X_1, \dots, X_k

матрицю M , а із стовпчиків X'_1, \dots, X'_k матрицю C . Як неважко зрозуміти, $C = AM$ і $M = A'C$. Якщо матриця C оборотна, то звідси зразу можна визначити дешифруючий ключ $A' = MC^{-1}$. Якщо суперникові пощастить менше і матриця C виявиться необоротною, то він не зможе визначити A' однозначно. Однак кількість можливостей може зменшитись настільки, що A' вдасться знайти після деякого перебору.

Для афінного шифру $E(X) = AX + S$ необхідно знати на одну пару (X, X') , де $X' = E(X)$, більше. Віднявши рівність $AX + S = X'$ від кожної з рівностей $AX_i + S = X'_i$, $i \leq k$, ми зведемо задачу визначення дешифруючого ключа до попереднього випадку.

Криптоаналіз

Атака лише за криптотекстом. Афінний шифр 2-го порядку піддається частотному аналізу як і будь-який біграмний шифр. Якщо порядок k дещо збільшити, частотний метод перестане працювати.

Розглянемо лінійний шифр k -го порядку над алфавітом \mathbb{Z}_n . Подивимось, які перспективи може мати брутальна атака, іншими словами, наскільки реально влаштувати повний перебір ключів. Очевидно, кількість ключів дорівнює кількості матриць в $GL_k(\mathbb{Z}_n)$, для якої в пункті 2.5 було введено позначення $\phi_k(n)$. Там же була виведена формула $\phi_k(n) = n^{k^2} \prod_{p|n} \prod_{i=1}^k (1 - 1/p^i)$. З одного боку видно, що $\phi_k(n) \leq n^{k^2}$. З іншого, порівнюючи із формулою для функції Ойлера $\phi(n) = \phi_1(n)$, отримуємо $\phi_k(n) \geq n^{k^2-k} (\phi(n))^k$. З використанням твердження 2.15 маємо оцінку $\phi_k(n) \geq n^{k^2} / (6 \ln \ln n)^k$ при $n > 4$. Асимптотично, значення $\phi_k(n)$ зростає за n як поліном і за k як експоненційна функція. Отримана оцінка дозволяє оцінити розмір простору ключів для будь-яких конкретних k і n (див. також вправу 3.20). Як видно, перебір ключів напевне є нереальним скажімо при $k = 5$, $n = 32$. Платою за збільшення порядку шифру є збільшення часу криптування і декриптування.

Криптоаналіз

Вправа для самостійного виконання:

Перехоплене повідомлення отримане за допомогою лінійного шифру 3-го порядку над 33-літерним алфавітом (пропуски між словами ігноруються):

ЕЬЩИЦЕШЩДНІТЛЧТХХИШХКПСГТНВТУ

Повідомлення закінчується підписом:

ДЖЕЙМСБОНД

що дає можливість встановити відповідність між трьома триграмами повідомлення і криптотексту. Знайти дешифруючий ключ і прочитати повідомлення.

