

Класичні шифри

У пошуках математики

Сергій Яковлєв

кафедра математичних методів захисту інформації,
НН ФТІ КПІ ім. Ігоря Сікорського
yasv@rl.kyiv.ua



- ① Шифросистеми та класичні шифри
- ② Шифр частоколу
- ③ Загальний шифр табличної перестановки
- ④ Ґратка Кардано

- 1 Шифросистеми та класичні шифри
- 2 Шифр частоколу
- 3 Загальний шифр табличної перестановки
- 4 Ґратка Кардано

Шифросистема (дуже неформальне означення)

- Три множини: відкритих текстів (повідомлень), шифротекстів та ключів
 - ▷ Текстами зазвичай є послідовності символів, ключами може бути що завгодно
- Три алгоритми: шифрування E_K , розшифрування D_K , вироблення ключів

Шифросистема (дуже неформальне означення)

- Три множини: відкритих текстів (повідомлень), шифротекстів та ключів
 - ▷ Текстами зазвичай є послідовності символів, ключами може бути що завгодно
- Три алгоритми: шифрування E_K , розшифрування D_K , вироблення ключів
- Два обмеження:
 - Різні відкриті тексти шифруються одним ключем у різні шифротексти
 - Однозначність розшифрування: $D_K(E_K(X)) = X$ для довільних X та K

Класичні шифри

Класичні шифри — усі шифросистеми, створені до 1949 року

- ❑ Шифри перестановки (*permutation ciphers*): зміна позицій символів у тексті
- ❑ Шифри підстановки (заміни) (*substitution ciphers*): зміна позначень символів
 - моноалфавітні шифри: правило заміни однакове для будь-якої позиції у тексті
 - поліалфавітні шифри: правило заміни залежить від позиції у тексті
- ❑ Комбіновані шифри: перестановка + підстановка



- ① Шифросистеми та класичні шифри
- ② Шифр частоколу
- ③ Загальний шифр табличної перестановки
- ④ Ґратка Кардано

Шифр частоколу

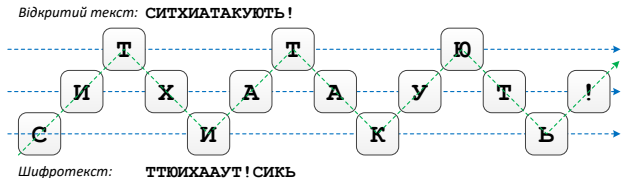
Шифр частоколу — один з перших задокументованих шифрів (≈ 300 р. до н.е.)

Шифрування:

- Текст записується зигзагом («частоколом»)
- Шифротекст зчитується рядочками
- Ключем є висота частоколу h

Розшифрування:

дії виконуються в зворотному порядку



Шифр частоколу

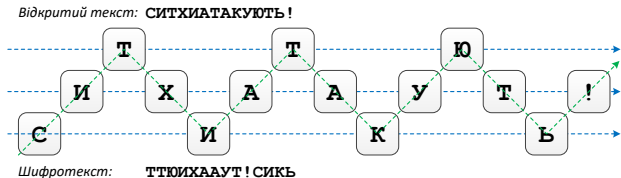
Шифр частоколу — один з перших задокументованих шифрів (≈ 300 р. до н.е.)

Шифрування:

- Текст записується зигзагом («частоколом»)
- Шифротекст зчитується рядочками
- Ключем є висота частоколу h

Розшифрування:

дії виконуються в зворотному порядку

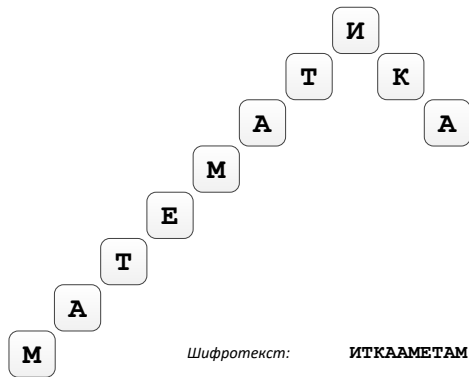


Властивості:

- Один з небагатьох шифрів, чутливих до довжини відкритого тексту
- Ламається **методом повного перебору**: треба перебрати усього L кандидатів у ключі, де L — довжина шифротексту

Шифр частоголу: на великій висоті

- Пошук ключа можна прискорити: якщо висота частоголу співставна з довжиною тексту, то шифротексти мають характерну особливість :)

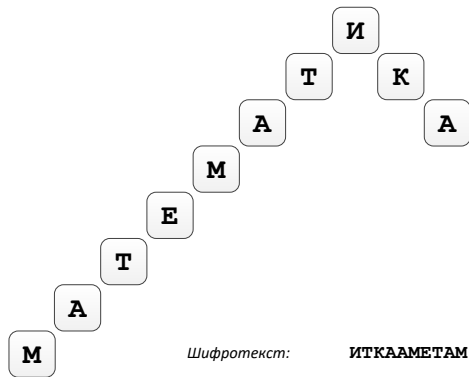


Шифр частоколу: на великій висоті

□ Пошук ключа можна прискорити: якщо висота частоколу співставна з довжиною тексту, то шифротексти мають характерну особливість :)

⇒ Тому перед тим, як перебирати ключі, спочатку прочитайте текст назворот

- Якщо склалось у щось змістовне — висота відносно велика
- Якщо не склалось — висота невелика



Шифр частоту: ітеративне шифрування

Зашифруємо слово «ПАРКАН» шифром частоту висоти 4: ПАРКАН → КРААНП

Шифр частотолу: ітеративне шифрування

Зашифруємо слово «ПАРКАН» шифром частотолу висоти 4: ПАРКАН → КРААНП
Зашифруємо ще раз :)

- 1 ПАРКАН → КРААНП
- 2 КРААНП → ААНРПК
- 3 ААНРПК → РНПАКА
- 4 РНПАКА → АПКНАР
- 5 АПКНАР → НКАПРА

Шифр частотолу: ітеративне шифрування

Зашифруємо слово «ПАРКАН» шифром частотолу висоти 4: ПАРКАН → КРААНП
Зашифруємо ще раз :)

- 1 ПАРКАН → КРААНП
- 2 КРААНП → ААНРПК
- 3 ААНРПК → РНПАКА
- 4 РНПАКА → АПКНАР
- 5 АПКНАР → НКАПРА
- 6 НКАПРА → ПАРКАН

Шифр частотолу: ітеративне шифрування

Зашифруємо слово «ПАРКАН» шифром частотолу висоти 4: ПАРКАН → КРААНП
Зашифруємо ще раз :)

- ① ПАРКАН → КРААНП
- ② КРААНП → ААНРПК
- ③ ААНРПК → РНПАКА
- ④ РНПАКА → АПКНАР
- ⑤ АПКНАР → НКАПРА
- ⑥ НКАПРА → ПАРКАН

Питання, які повинні виникнути:

- Так завжди відбувається? (Це випадковість чи закономірність?)
- Скільки разів треба шифрувати?

Чому це відбувається?

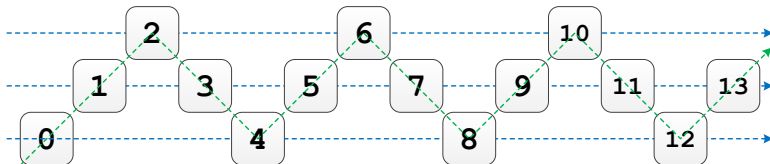
- Повідомлень з n символів скінченна кількість, а шифрувати ми можемо до нескінченності
- ⇒ За принципом Діріхле рано чи пізно шифротексти почнуть повторюватись

Чому це відбувається?

- Повідомлень з n символів скінченна кількість, а шифрувати ми можемо до нескінченності
- ⇒ За принципом Діріхле рано чи пізно шифротексти почнуть повторюватись
- [?] Але чому шифрування замкнеться на початок, а не повториться десь на проміжному шифротексті?
- Якщо повтор відбудеться не на початку, це означатиме, що два різних повідомлення зашифрувались в один шифротекст
- ⇒ А це порушує властивість однозначного розшифрування

Шифр частоголу: підрахунок кількості ітерацій

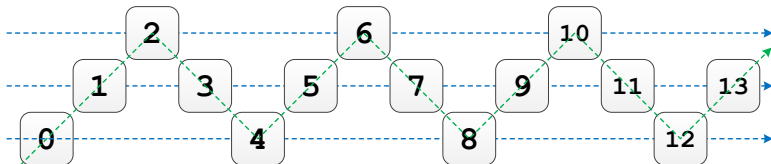
Для повідомлення довжини $L = 14$ частогол висоти 3 задає таку перестановку:



$$\pi = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 \\ 2 & 6 & 10 & 1 & 3 & 5 & 7 & 9 & 11 & 13 & 0 & 4 & 8 & 12 \end{pmatrix} = \\ = (0 \ 2 \ 10)(1 \ 6 \ 7 \ 9 \ 13 \ 12 \ 8 \ 11 \ 4 \ 3)(5)$$

Шифр частоголу: підрахунок кількості ітерацій

Для повідомлення довжини $L = 14$ частогол висоти 3 задає таку перестановку:



$$\begin{aligned}\pi &= \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 \\ 2 & 6 & 10 & 1 & 3 & 5 & 7 & 9 & 11 & 13 & 0 & 4 & 8 & 12 \end{pmatrix} = \\ &= (0\ 2\ 10)(1\ 6\ 7\ 9\ 13\ 12\ 8\ 11\ 4\ 3)(5)\end{aligned}$$

- ▷ Перестановка π розпадається на цикли довжини 3, 10 та 1
- ▷ **Порядок π :** $T = \text{lcm}(3, 10, 1) = 30$ (тобто, за 30 ітерацій π стає тотожною)
- ⇒ за 29 ітерацій шифротекст перейде у відкритий текст

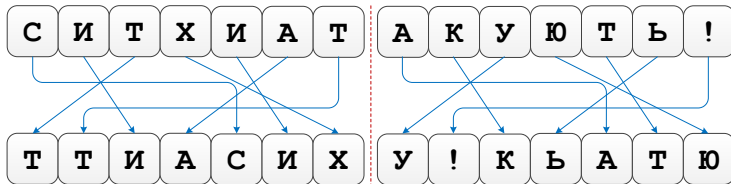
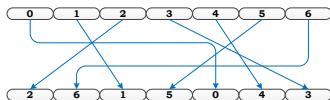
- ① Шифросистеми та класичні шифри
- ② Шифр частоколу
- ③ Загальний шифр табличної перестановки
- ④ Ґратка Кардано

Загальний шифр табличної перестановки — модель, яка описує більшість відомих шифрів перестановки

- Відкритий текст розбивається на блоки по n символів
- Ключем є перестановка номерів від 0 до $n - 1$ (або від 1 до n , якщо так зручніше :))
 - ▷ Зазвичай задається табличкою, звідки й назва
- Шифрування — застосування перестановки до кожного блоку
- Розшифрування — застосування оберненої перестановки до кожного блоку

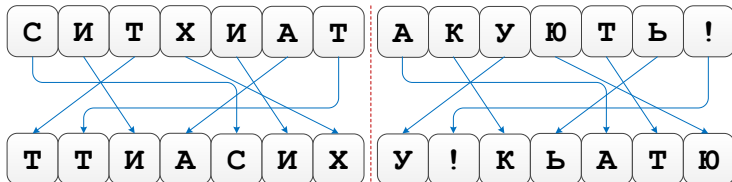
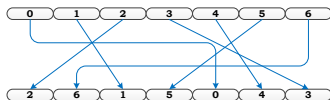
Загальний шифр табличної перестановки: приклад

$$\pi = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 6 & 1 & 5 & 0 & 4 & 3 \end{pmatrix}$$



Загальний шифр табличної перестановки: приклад

$$\pi = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 6 & 1 & 5 & 0 & 4 & 3 \end{pmatrix}$$



Кількість ключів: $|\mathcal{K}| = n!$; можна оцінити за формулою Стірлінга: $n! \sim \sqrt{2\pi n} \cdot (n/e)^n$

- $n = 10$: $|\mathcal{K}| \approx 2^{21.79}$
- $n = 15$: $|\mathcal{K}| \approx 2^{40.25}$
- $n = 20$: $|\mathcal{K}| \approx 2^{61.08}$ — на межі обчислювальної потужності планети Земля
- $n = 25$: $|\mathcal{K}| \approx 2^{83.68}$ — за межами повного перебору

Загальний шифр табличної перестановки: паддінг

Проблема: Тексти треба вирівнювати по довжині блоку

▷ Як тоді доповнювати останній блок?

Загальний шифр табличної перестановки: паддінг

Проблема: Тексти треба вирівнювати по довжині блоку

▷ Як тоді доповнювати останній блок?

Приклад: будемо доповнювати текст спеціальними символами «*» (зірочками)

Нехай у блоку є r зірочок. Скільки тепер ключів буде перебирати аналітик?

Загальний шифр табличної перестановки: паддінг

Проблема: Тексти треба вирівнювати по довжині блоку

▷ Як тоді доповнювати останній блок?

Приклад: будемо доповнювати текст спеціальними символами «*» (зірочками)

Нехай у блоку є r зірочок. Скільки тепер ключів буде перебирати аналітик?

□ □ □ □ □ * *

Р * І * З А К

Загальний шифр табличної перестановки: паддінг

Проблема: Тексти треба вирівнювати по довжині блоку

▷ Як тоді доповнювати останній блок?

Приклад: будемо доповнювати текст спеціальними символами «*» (зірочками)

Нехай у блоку є r зірочок. Скільки тепер ключів буде перебирати аналітик?



☐ Зірки, очевидно, повинні стояти в кінці блоку

☐ Варіантів переставити зірки: $r!$

Варіантів переставити інші літери: $(n - r)!$

⇒ Разом $r!(n - r)!$ варіантів

Загальний шифр табличної перестановки: паддінг

Проблема: Тексти треба вирівнювати по довжині блоку

▷ Як тоді доповнювати останній блок?

Приклад: будемо доповнювати текст спеціальними символами «*» (зірочками)

Нехай у блоку є r зірочок. Скільки тепер ключів буде перебирати аналітик?



☐ Зірки, очевидно, повинні стояти в кінці блоку

☐ Варіантів переставити зірки: $r!$

Варіантів переставити інші літери: $(n - r)!$

⇒ Разом $r!(n - r)!$ варіантів

Мінімальне значення для аналітика: $\frac{r!(n - r)!}{n!} = \frac{1}{C_n^r}$

• Максимальний біноміальний коефіцієнт — центральний $\Rightarrow r = \lfloor n/2 \rfloor$

▷ Будуємо трикутник Паскаля, щоб переконатись :)

▷ А потім доводимо строго через відношення C_n^{k+1}/C_n^k

Загальний шифр табличної перестановки: якість перестановок

Проблема: Не всі перестановки однаково гарно приховують зміст
Зашифруйте щось такими перестановками:

$$\pi = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ 0 & 1 & 2 & 3 & 4 & 6 & 5 \end{pmatrix} \quad \pi = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 & 0 \end{pmatrix}$$

Але й нема чітких формальних критеріїв «гарності» перестановки!

Подумайте разом, які можуть бути вимоги до «гарної» перестановки?

Загальний шифр табличної перестановки: гармидери

Приклад: Нехай жодна літера блоку не залишається на своєму місці!

Гармидер (*disorder*) — перестановка без нерухомих точок

Загальний шифр табличної перестановки: гармидери

Приклад: Нехай жодна літера блоку не залишається на своєму місці!

Гармидер (*disorder*) — перестановка без нерухомих точок

□ Кількість гармидерів рахується за формулою включень та виключень:

$$D_n = n! - C_n^1(n-1)! + C_n^2(n-2)! - \dots + (-1)^n C_n^n 0! = \sum_{k=1}^n (-1)^k \frac{n!}{k!}$$

- ▷ Віднімаємо кількість перестановок, у яких є нерухома точка: обираємо нерухому точку (C_n^1 способів), переставляємо інші елементи довільним чином ($(n-1)!$ способів)
- ▷ Перестановки з двома нерухомими точками відняли двічі → повертаємо назад
- ▷ Перестановки з трьома нерухомими точками тричі відняли і тричі повернули → треба знову віднімати...

Загальний шифр табличної перестановки: гармидери

Приклад: Нехай жодна літера блоку не залишається на своєму місці!

Гармидер (*disorder*) — перестановка без нерухомих точок

- Кількість гармидерів рахується за формулою включень та виключень:

$$D_n = n! - C_n^1(n-1)! + C_n^2(n-2)! - \dots + (-1)^n C_n^n 0! = \sum_{k=1}^n (-1)^k \frac{n!}{k!}$$

- ▷ Віднімаємо кількість перестановок, у яких є нерухома точка: обираємо нерухому точку (C_n^1 способів), переставляємо інші елементи довільним чином $((n-1)!$ способів)
- ▷ Перестановки з двома нерухомими точками відняли двічі → повертаємо назад
- ▷ Перестановки з трьома нерухомими точками тричі відняли і тричі повернули → треба знову віднімати...

- Оцінка: $D_n \approx n!/e$

- Кількість перестановок з r нерухомими точками: $D_{n,r} = C_n^r D_{n-r} \approx n!/(r!e)$

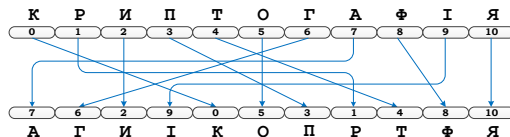
Загальний шифр табличної перестановки: вироблення ключів

Як запам'ятати ключ-перестановку?

▷ в суворе Середньовіччя люди ще не знали абстрактної алгебри...

Метод генерування перестановок (для людей)

- Обирається довільне слово (пароль): «КРИПТОГРАФІЯ»
- Зі слова викидаються дублікати літер: «КРИПТОГ**Р**АФІЯ» → «КРИПТОГАФІЯ»
- Літери сортуються в алфавітному порядку



⇒ Перестановка готова

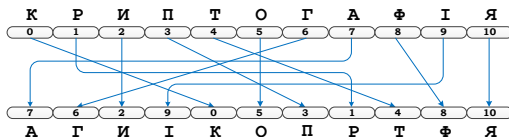
Загальний шифр табличної перестановки: вироблення ключів

Як запам'ятати ключ-перестановку?

- ▷ в суворе Середньовіччя люди ще не знали абстрактної алгебри...

Метод генерування перестановок (для людей)

- Обирається довільне слово (пароль): «КРИПТОГРАФІЯ»
- Зі слова викидаються дублікати літер: «КРИПТОГ**Р**АФІЯ» → «КРИПТОГАФІЯ»
- Літери сортуються в алфавітному порядку



⇒ Перестановка готова

- ▷ Але, як каже нам теорія інформації, кількість таких перестановок **значно** менше, ніж видається
- ▷ Порівняйте кількість слів у словнику із загальною кількістю перестановок

Загальний шифр табличної перестановки: вироблення ключів

Спробуйте придумати алгоритми, які б породжували ключі-перестановки, та порівняйте їх між собою

Спробуйте придумати алгоритми, які б породжували ключі-перестановки, та порівняйте їх між собою

Генерування випадкових перестановок: **алгоритм Фішера-Єтса**

- ❶ Обирається довільний елемент з $0, 1, \dots, n - 1$ і ставиться на перше місце
- ❷ Обирається довільний елемент з тих, які залишились, і ставиться на друге місце
- ❸ Обирається довільний елемент з тих, які залишились, і ставиться на третє місце
- ...
- ▷ Останній необраний елемент ставиться на останню позицію

Загальний шифр табличної перестановки: вироблення ключів

Спробуйте придумати алгоритми, які б породжували ключі-перестановки, та порівняйте їх між собою

Генерування випадкових перестановок: **алгоритм Фішера-Етса**

- 1 Обирається довільний елемент з $0, 1, \dots, n - 1$ і ставиться на перше місце
- 2 Обирається довільний елемент з тих, які залишились, і ставиться на друге місце
- 3 Обирається довільний елемент з тих, які залишились, і ставиться на третє місце

...

▷ Останній необраний елемент ставиться на останню позицію

Будь-яка перестановка породжується цим алгоритмом з однаковою імовірністю

- Імовірність, що співпадає перший елемент: $1/n$
- Імовірність, що співпадає другий елемент: $1/(n - 1)$ і так далі

⇒ Разом виходить $1/n!$

- ① Шифросистеми та класичні шифри
- ② Шифр частоколу
- ③ Загальний шифр табличної перестановки
- ④ Гратка Кардано

Ґратка Кардано (*Cardan grille*) — загальна назва декількох різних методів шифрування та шифрувальних пристроїв, створених у XVI-XIX ст.

- ❑ Первинно — стеганографічний метод: приховування справжнього повідомлення всередині шуму



- У трафареті вирізались випадкові дірки
- Потрібний текст вписувався в дірки
 - ▷ по словах чи навіть по літерах
- Простір, що залишався, заповнювався довільним зв'язним текстом на геть іншу тему, який обгортав та приховував справжнє повідомлення



Gerolamo Cardano
(1501–1576)

- ▷ Цей метод вимагав нетривіальних літературних навичок
- ❑ В подальшому ґратка Кардано перетворилась у чесний шифрувальний пристрій

Ґратка Кардано: опис

- Ґратка $2n \times 2n$ розбивається на чотири частини;
клітинки нумеруються числами від 1 до n^2
 - ▷ Однакові номери у клітинок, які співпадають при поворотах навколо центру
- Із ґратки вирізається по одній клітинці кожного номера

1	2	3	7	4	1
4	5	6	8	5	2
7	8	9	9	6	3
3	6	9	9	8	7
2	5	8	6	5	4
1	4	7	3	2	1

		3			1
4					
			9		
	6			8	
2				5	
		7			

Ґратка Кардано: опис

- Ґратка $2n \times 2n$ розбивається на чотири частини; клітинки нумеруються числами від 1 до n^2
 - ▷ Однакові номери у клітинок, які співпадають при поворотах навколо центру
- Із ґратки вирізається по одній клітинці кожного номера

1	2	3	7	4	1
4	5	6	8	5	2
7	8	9	9	6	3
3	6	9	9	8	7
2	5	8	6	5	4
1	4	7	3	2	1

		3			1
4					
			9		
	6			8	
2				5	
		7			

- Відкритий текст розбивається на блоки розміру $4n^2$
- Літери тексту вписуються у дірки ґратки зверху вниз, справа наліво
Потім ґратка повертається, вписуються наступні символи — і так ще два рази
- Шифротекст виписується по рядочках

Гратка Кардано: приклад та аналіз

СИТХ ИАТА КУЮТ Ъ!!!

			С
И		Т	
	Х		

Гратка Кардано: приклад та аналіз

СИТХ ИАТА КУЮТ Ъ!!!

			С
И		Т	
	Х		

СИТХ ИАТА КУЮТ Ъ!!!

	И		С
А			
И	Т	Т	
	Х		А

Гратка Кардано: приклад та аналіз

СИТХ ИАТА КУЮТ Ъ!!!

			С
И		Т	
	Х		

СИТХ ИАТА КУЮТ Ъ!!!

	И		С
А			
И	Т	Т	
	Х		А

СИТХ ИАТА КУЮТ Ъ!!!

	И	К	С
А	У		Ю
И	Т	Т	
Т	Х		А

Гратка Кардано: приклад та аналіз

СИТХ ИАТА КУЮТ Ъ!!!

			С
И		Т	
	Х		

СИТХ ИАТА КУЮТ Ъ!!!

	И		С
А			
И	Т	Т	
	Х		А

СИТХ ИАТА КУЮТ Ъ!!!

	И	К	С
А	У		Ю
И	Т	Т	
Т	Х		А

СИТХ ИАТА КУЮТ Ъ!!!

Ь	И	К	С
А	У	!	Ю
И	Т	Т	!
Т	Х	!	А

ЬИКСАУ!ЮИТТ!ТХ!А

Гратка Кардано: приклад та аналіз

СИТХ ИАТА КУЮТ Ъ!!!

			С
И		Т	
	Х		

СИТХ ИАТА КУЮТ Ъ!!!

	И		С
А			
И	Т	Т	
	Х		А

СИТХ ИАТА КУЮТ Ъ!!!

	И	К	С
А	У		Ю
И	Т	Т	
Т	Х		А

СИТХ ИАТА КУЮТ Ъ!!!

Ь	И	К	С
А	У	!	Ю
И	Т	Т	!
Т	Х	!	А

ЬИКСАУ!ЮИТТ!ТХ!А

□ Кількість ключів: існує $|\mathcal{K}| = 4^{n^2}$ ґраток розміру $2n \times 2n$

▷ Треба вирізати n^2 номерів-дірок, на кожен номер по 4 варіанти

- $n = 5$: $|\mathcal{K}| = 2^{50}$
- $n = 7$: $|\mathcal{K}| = 2^{98}$ — за межами повного перебору

Гратка Кардано: приклад та аналіз

СИТХ ИАТА КУЮТ Ъ!!!

			С
И		Т	
	Х		

СИТХ ИАТА КУЮТ Ъ!!!

	И		С
А			
И	Т	Т	
	Х		А

СИТХ ИАТА КУЮТ Ъ!!!

	И	К	С
А	У		Ю
И	Т	Т	
Т	Х		А

СИТХ ИАТА КУЮТ Ъ!!!

Ь	И	К	С
А	У	!	Ю
И	Т	Т	!
Т	Х	!	А

ЬИКСАУ!ЮИТТ!ТХ!А

- Кількість ключів: існує $|\mathcal{K}| = 4^{n^2}$ ґраток розміру $2n \times 2n$
 - ▷ Треба вирізати n^2 номерів-дірок, на кожен номер по 4 варіанти
 - $n = 5$: $|\mathcal{K}| = 2^{50}$
 - $n = 7$: $|\mathcal{K}| = 2^{98}$ — за межами повного перебору
- Великі блоки ($n = 5$: блок у 100 символів) $\Rightarrow$ проблема вирівнювання довжини
Але: так у аналітика менше інформації для зламу

- Що буде, якщо вирівнювати повідомлення зірочками?
 - ▷ Кожна зірочка «зливає» позицію однієї дірки на ґратці
 - ▷ n^2 зірочок дозволяють відновити ґратку повністю

- Що буде, якщо вирівнювати повідомлення зірочками?
 - ▷ Кожна зірочка «зливає» позицію однієї дірки на ґратці
 - ▷ n^2 зірочок дозволяють відновити ґратку повністю
- Як побудувати ґратку непарного розміру $(2n + 1) \times (2n + 1)$?
 - ▷ І що робити з центральною клітинкою?
- Як побудувати прямокутну ґратку $2n \times 2m$?
 - ▷ Пограйтесь в симетрії!



Дякую за увагу!

<https://mmis.ipt.kpi.ua>

https://youtube.com/mmis_ipt