

Ідеальний шифр. Чи існує він?

# Шифр Вернама

- 1917 рік – співробітники компанії AT&T Гілберт Вернам та Джозеф Моборн розробили метод шифрування з нескінченною стрічкою.
- Літери відкритого тексту додавалися за правилами XOR з літерами ключової стрічки, довжина якої завжди була рівною довжині повідомлення.
- Вернам використовував кожну стрічку лише один раз, а потім знищував її.
- 1919 рік – отримано патент на цей спосіб шифрування.
- Шифр Вернама – єдиний шифр, для якого теоретично доведено абсолютну криптографічну стійкість.

# Що це значить?

- Теоретично: шифр буде ідеально стійким, якщо апріорна ймовірність отримання інформації (тобто до її розшифрування) дорівнює апостеріорній ймовірності (тобто після її розшифрування).
- Статистично: якщо детерміновану величину об'єднати з випадковою, то результат буде випадковим.
- Як реалізувати таке шифрування?

# Приклад шифру Вернама

- Припустимо, що нам треба передати у військо повідомлення: *«наказую відступати»*.
- Використаємо таку таблицю заміни:

А	Б	В	Г	Д	Е	Є	Ж	З	И	І	Ї	Й	К	Л	М
00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15
Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ю	Я
16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31

# Приклад шифру Вернама

- Згенеруємо випадковий ключ однакової з повідомленням довжини (18 символів):

10	30	01	17	26	13	01	09	04	21	12	05	19	21	00	27	14	18
----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----

- Повідомлення перетворимо так:  
«наказую~~ф~~відступати»
- Замінімо літери повідомлення цифрами згідно таблиці заміни:

16	00	13	00	08	22	30	23	02	10	04	20	21	22	18	00	21	09
----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----

# Приклад шифру Вернама

- Тепер додамо цифри повідомлення і ключа за правилами  $\text{mod } 32$ . Отримаємо:

16	00	13	00	08	22	30	23	02	10	04	20	21	22	18	00	21	09
10	30	01	17	26	13	01	09	04	21	12	05	19	21	00	27	14	18
26	30	14	17	02	03	31	00	06	31	16	25	08	11	18	27	03	27

- Цю шифрограму передаємо у військово каналами зв'язку.
- Отримавши повідомлення, шифрувальник розшифровує повідомлення, віднімаючи від нього ключ за правилами  $\text{mod } 32$ :

# Приклад шифру Вернама

- Отримає:

26	30	14	17	02	03	31	00	06	31	16	25	08	11	18	27	03	27
10	30	01	17	26	13	01	09	04	21	12	05	19	21	00	27	14	18
16	00	13	00	08	22	30	23	02	10	04	20	21	22	18	00	21	09
Н	А	К	А	З	У	Ю	Ф	В	І	Д	С	Т	У	П	А	Т	И

- Замінивши коди літерами, отримуємо повідомлення.
- Таким чином, ми розшифрували повідомлення: *«наказую відступати»*.

# Приклад шифру Вернама

- Зловмисник не знає ключа, на якому шифрувалося повідомлення!
- Перехопивши повідомлення, знаючи, що використовувався шифр Вернама, він буде підставляти усі можливі ключі шифрування.
- Якщо він підставить наш використаний ключ, він отримає розшифроване повідомлення: *«наказуюфвідступати»*.



# Приклад шифру Вернама

Якщо він підставить ключ:

10	30	01	17	26	13	01	09	22	31	28	04	18	25	18	06	26	04
----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----

Він отримає таке повідомлення:

26	30	14	17	02	03	31	00	06	31	16	25	08	11	18	27	03	27
10	30	01	17	26	13	01	09	22	31	28	04	18	25	18	06	26	04
16	00	13	00	08	22	30	23	16	00	20	21	22	18	00	21	09	23
Н	А	К	А	З	У	Ю	Ф	Н	А	С	Т	У	П	А	Т	И	Ф

«наказую~~ф~~наступати~~ф~~»

# Приклад шифру Вернама

Якщо ж він підставить ключ:

10	25	11	17	22	19	14	09	30	27	16	23	08	31	29	22	15	28
----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----

Він отримає таке повідомлення:

26	30	14	17	02	03	31	00	06	31	16	25	08	11	18	27	03	27
10	25	11	17	22	19	14	09	30	27	16	23	08	31	29	22	15	28
26	30	14	17	02	03	31	00	06	31	16	25	08	11	18	27	03	27
Н	Е	Г	А	Й	Н	О	Ф	З	Д	А	В	А	Й	Т	Е	С	Я

«негайно~~ф~~здавайтесь»

# Приклад шифру Вернама

- Зловмисник може отримати ще багато інших логічно зв'язаних текстів, тобто ВСІ МОЖЛИВІ ТЕКСТИ ДОВЖИНОЮ ДО 18 СИМВОЛІВ!
- Розглянемо отримані три тексти:
  - *«наказую відступати»;*
  - *«наказую наступати»;*
  - *«негайно здавайтеся».*

Який з них правильний?

Як це визначити?

# Приклад шифру Вернама

- Для вибору правильного повідомлення зломисник повинен володіти ще якоюсь додатковою інформацією.
- Такою інформацією для супротивника може бути розвідувальна або агентурна інформація.
- Наприклад: якщо чисельність та озброєння військ супротивника кращі, ніж у нього, тоді найбільш ймовірно друге повідомлення;
- Якщо навпаки – перше, про відступ.
- Якщо військо супротивника деморалізоване – тоді останнє.

# Приклад шифру Вернама

- Уявимо, що ми знайшли цю шифровку через 100 років. Чи зможемо ми обрати правильне, те, яке є дійсно істинним повідомленням? Адже такої додаткової інформації у нас немає!
- У цьому сенсі говорять, що шифр Вернама і є ідеально стійким шифром.
- Розшифрувати його можна, але ми одержимо таку кількість відкритих текстів, що не зможемо вибрати з них істинне повідомлення.

# Умови застосування шифру Вернама

- Ключ шифрування повинен бути повністю випадковим;
- Довжина ключа шифрування повинна дорівнювати довжині повідомлення;
- Ключ повинен використовуватися лише один раз.

=====

Чому ж не використовують ідеальний шифр?  
Навіщо придумали інші шифри, якщо вони не ідеальні?

# Чому не використовують шифр Вернама?

- Використовують для особливо важливих випадків.
- Недоліки:
  - Проблема передавання ключа для розшифрування;
  - Проблема зберігання ключа.
- Приклади:
  - Одноразова стрічка;
  - Одноразовий блокнот.