Шифр перестановки

Шифр перестановки это

$(\Sigma^n, \Sigma^n, S_n, E, D)$

Где:

- S_n - это все перестановки длины n

Открытый текст m $= m_1 m_2 ... m_n$

Криптограмма c $= c_1 c_2 ... c_n$

$k \in S_n$ такое что $k : \{1, 2...n\} \to \{1, 2...n\}$(эта стрелка обозначает биекцию, в латехе нет таких стрелок блять)

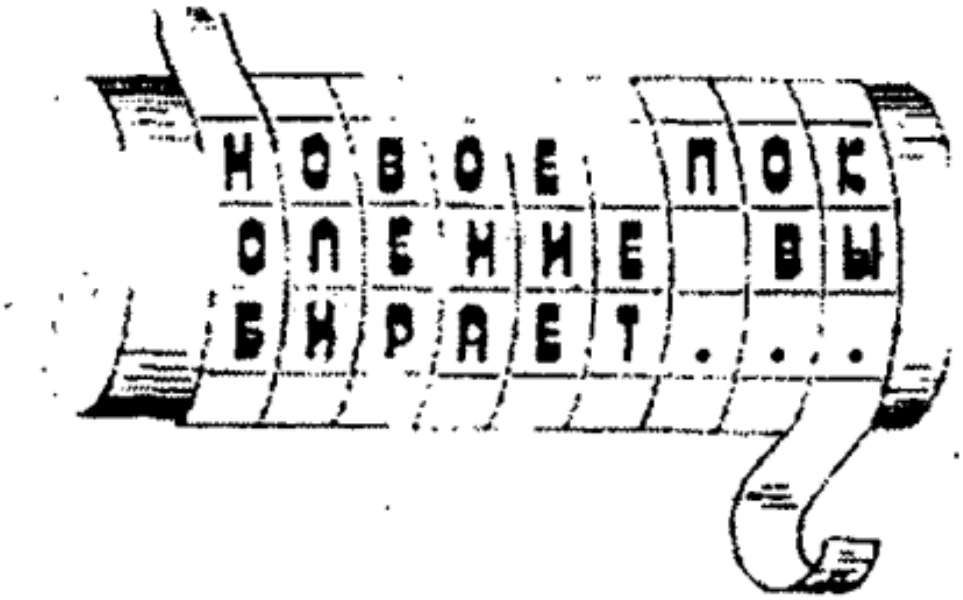
$E(m, k) = c$ по правилу $c_i = m_{k(i)}$где $j = k(i)$

$D(c, k) = m$ по правилу $m_i = c_{k^{-1}(i)}$где $i = k^{-1}(i)$

Исторические шифры перестановки

Шифр Сцитала

Одним из первых физических приборов, реализующих шифр перестановки, является так называемый прибор Сцитала. Он был изобретён в древней «варварской» Спарте во времена Ликурга (V в. до н. э.). Рим быстро воспользовался этим прибором. Для зашифрования текста использовался цилиндр заранее обусловленного диаметра. На цилиндр наматывался тонкий ремень из пергамента, и текст выписывался построчно по образующей цилиндра (вдоль его оси). Затем ремень сматывался и отправлялся получателю сообщения. Последний наматывал его на цилиндр того же диаметра и читал текст по оси цилиндра. В этом примере ключом шифра являлся диаметр цилиндра и его длина, которые, по существу, порождают двухстрочную запись, аналогичную указанной выше.

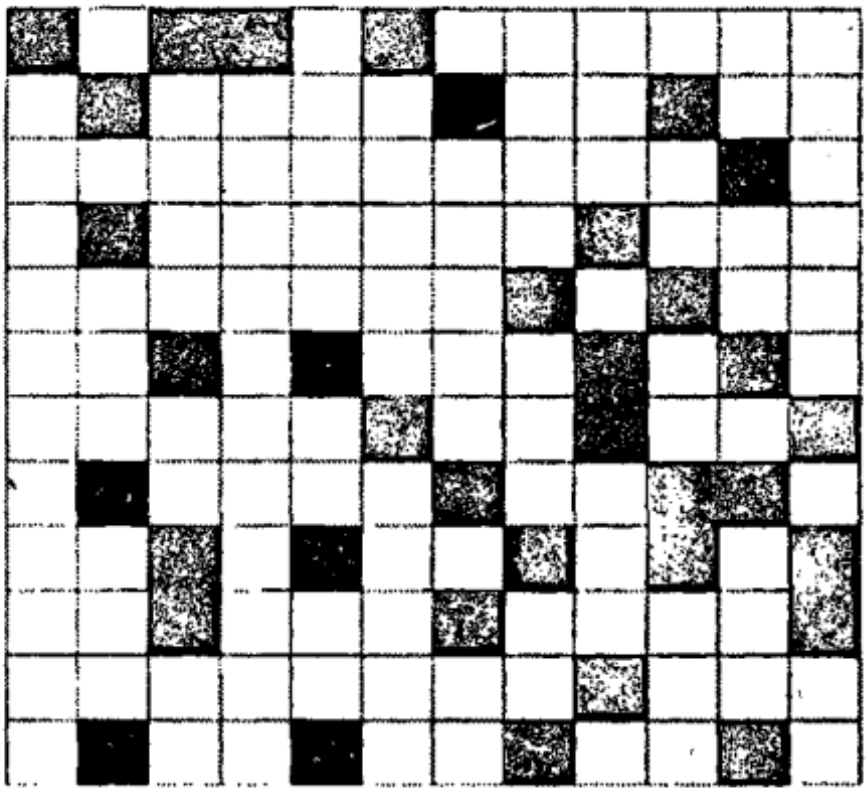


Изобретение дешифровального устройства – «Антисцитала» – приписывается великому Аристотелю. Он предложил использовать конусообразное «копьё», на которое наматывался перехваченный ремень; этот ремень передвигался по оси до того положения, пока не появлялся осмысленный текст.

ром имеются разделы, посвященные криптографии. В ней нашли отражение новые идеи криптографии: использование части самого передаваемого открытого текста в качестве ключа шифра и новый способ шифрования, который вошел в историю как «решетка Кардано». Для ее изготовления брался лист из твердого материала (картон, пергамент, металл), представляющий собой квадрат, в котором вырезаны «окна». При шифровании решетка накладывалась на лист бумаги, и буквы открытого текста вписывались в «окна». При использовании всех «окон» решетка поворачивалась на 90 градусов, и вновь буквы открытого текста вписывались в «окна» повернутой решетки. Затем вновь производился поворот на 90 градусов и т. д. В один «заход» решетка работала 4 раза. Если текст зашифрован не полностью, то решетка ставилась в исходное положение и вся процедура повторялась. Это ничто иное, как шифр перестановки.

Главное требование к решетке Кардано – при всех поворотах «окна» не должны попадать на одно и то же место в квадрате, в котором образуется шифртекст.

Если в квадрате после снятия решетки образовывались пустые места, то в них вписывались произвольные буквы. Затем буквы квадрата выписывались построчно, что и было шифрованным текстом.



Квадрат Кардано

Про криптоанализ

Находимся в условиях, когда криптоаналитик знает какую криптосистему мы используем, но он не знаетключ

ОПР

Атака - Совокупность условий, в которых находится крипто аналитик называется атакой

Виды атак и методы атак

Виды атак:

1. **С известным шифротекстом**. Мы имеем доступ к зашифрованному сообщению и взлом осуществляется с помощью его исследования
2. **С известным открытым текстом**. Известны пары открытого текста и шифр текста
3. **С наиболее вероятным словом**, т.е знаем, что в криптограмме обязательно содержится определенное слово

4. **С избранным открытым текстом**, т.е Атакующий может расшифровывать выбранные шифртексты (кроме целевого). Либо атакующий может шифровать фрагменты открытого текста

Методы атак:

1. **Brute-force attack** (Полный перебор) Суть: Перебор всех возможных ключей. Эффективность: Зависит от длины ключа (например, 128-битный AES требует ~2^{12}⊠ попыток). Защита: Использование длинных ключей (256 бит и более).
2. **Частичная индукция**, т.е восстановление части открытого текста по криптограме
3. **Информационная индукция**, Получение некоторой инфы об открытом тексте по криптограме

Криптоанализ шифра перестановки

Атака№3(не устойчив к этой атаке)

можно по очереди зашифровать тексты вида:

- БАААА...А
- АБАА...А
- ААБА...А
- ...
- АААА...Б

глядя на эти тексты, мы узнаем куда перемещается буква Б, а также мы получим длину ключа,по образовавшимся периодам, таким образом получим ключ. Шифруем n раз, где n длина открытого текста

Также можно зашифровывать тексты вида

- АА..АББ..Б (первая половина состоит из букв А, вторая из букв Б)
- АА..АБ..ББАА..АБ..ББ(первая четверть из букв А, вторая из букв Б, третья снова из букв А, 4ая из букв Б)
- и тд

В итоге получим log(n) строк, с разными столбиками. Выясним, куда шифр перемещает iый столбик, тем самым поймем, куда перемещается iая буква из открытого текста

Атака №2(Взлом стал труднее, но ещё возможен)

По паре (m_i, c_i) находим часть ключевой перестановки, т.е множество перестановок, которые могут быть ключами, таким образом сокращая кол-во возможных перестановок. А потом перебор либо дополнение по осмысленности

Атака № 2'(Взлом стал труднее, но ещё возможен)

Подбираем кусок, в котором получается известное слово. Шифр перестановки не меняет множество букв, он просто переставляет их. Находим множество букв, из которых состоит нужное слово и пробуем переставлять их так, чтобы они оказались вместе. Далее подбираем ключ по осмысленности

Атака № 1

Перебор длины ключа. Перебираем n, начиная с 2 и далее во возрастанию.

После того как нашли длину ключа n, можно разделить зашифрованный текст по строчкам длины n и начинаем переставлять столбики, чтобы читался текст.

Чтобы сократить перебор, можно не рассматривать запрещенные или биграммы.Например Ъь, когда й стоит в начале слова. После того как выписали все запрещенные биграммы, то можем запретить стоять определенным столбикам друг за другом, иначе эта биграмма появится.

Таким образом построим таблицу запретов. Заполнив эту таблицу мы существенно сократим перебор