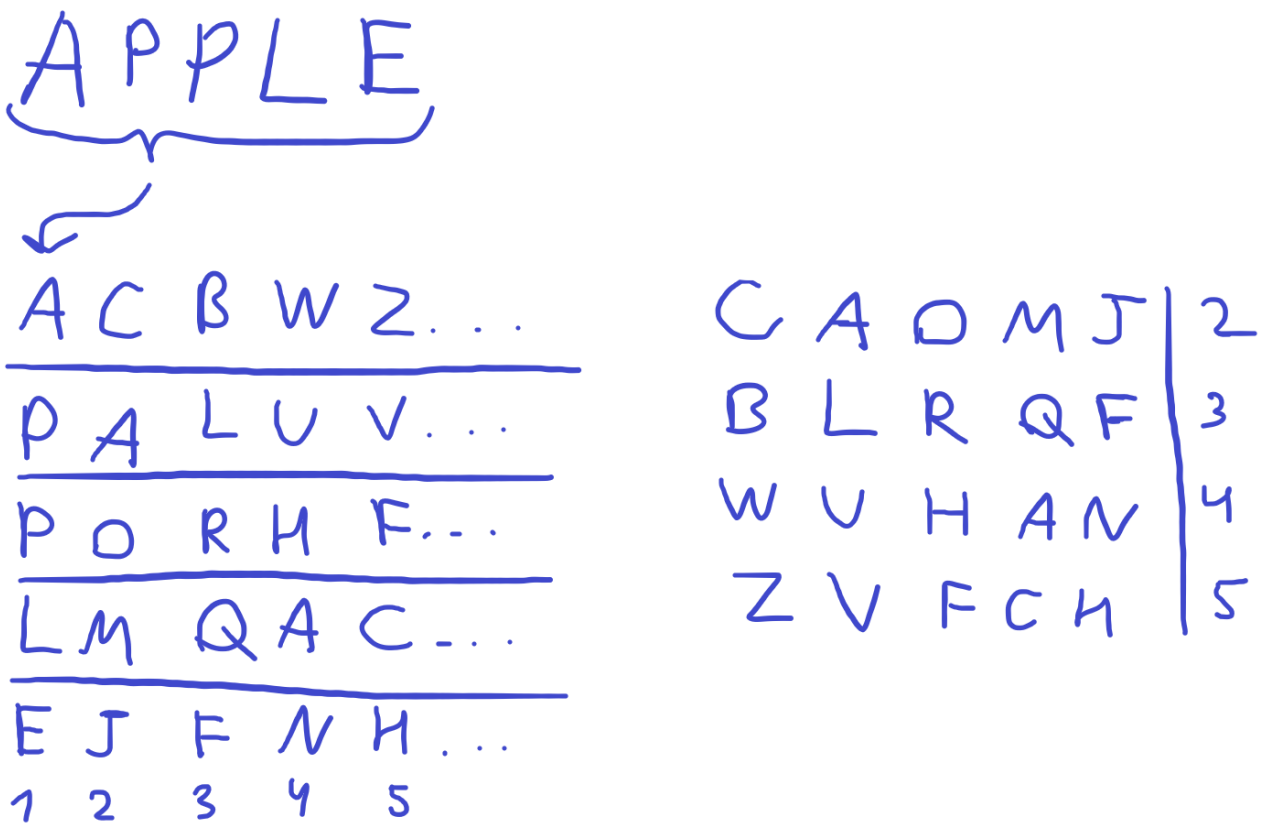
Дисковый шифратор Джефферсона и шифр Арджентри

Шифратор Джефферсона

Цилиндр Джефферсона — один из первых современных шифраторов, созданный Джефферсоном между 1790 г. и 1800 г. Джефферсон назвал свою систему шифрования «дисковым шифром». На момент создания устройство не получило большой популярности и довольно скоро попало в архив. В XX веке, когда изобретение нашли и вновь о нём вспомнили, оно было признано как очень стойкое к криптоанализу шифровальное устройство, а самого Джефферсона назвали «отцом американского шифровального дела».

Конструкция шифратора такова: деревянный цилиндр надет на ось и разрезан на 36 дисков, на каждый из этих дисков нанесен английский алфавит в произвольном порядке, диски могут вращаться независимо друг от друга. Над поверхностью цилиндра выделяется линия, под которой будет собираться открытый текст. Текст, который необходимо зашифровать разбивается на блоки по 36 символов. Первая буква блока находится на первом диске и фиксируется под выделенной линией, вторая — на следующем диске и т. д. Зашифрованный текст считывается с любой другой строки, кроме строки открытого текста. Расшифрование осуществляется на таком же шифраторе: шифротекст составляется под выделенной линией, открытый текст ищется среди параллельных линий, путём отыскания осмысленного сообщения. Количество ключей: $(25!)^{36} \cdot 36!$. Ключ - порядок расположения букв на каждом диске и порядок дисков.


APPLE
ACBWZ...
PALUV...
PORHF...
LMQAC...
EJFNH...
1 2 3 4 5
CAOMJ 2
BLRQF 3
WUHAN 4
ZVFCH 5

Достоинства шифра:

- Очень большое количество ключей
- Возможность замены ключа перестановкой цилиндров
- Даже при наличии шифровального устройства не получится расшифровать текст без знания ключа (ключом будет последовательность дисков - 36!)

Недостатки шифра:

Необходимость наличия шифратора для шифрования и расшифровки

Относительно долгий процесс шифрования и расшифровки

Шифр Ардженти

Шифр Ардженти, придуманный в 17 веке, является обычным шифром замены с дополнительными идеями: заменяются не только отдельные буквы, но и часто встречающиеся комбинации или даже слова, а также неоднозначность длины замен. Такой подход приводит к неоднозначности шифрования. Из одного текста могут быть получены различные шифр-тексты, возможно различной длины. Частотный анализ шифр-текста становится практически невозможным. Однако это все не влияет на сложность процесса расшифровки. Получателю достаточно последовательно просматривать шифр-текст и заменять его на символы из таблицы.

Пример алфавита шифрования:

Таблица 5. *Шифр Арджентти*

A	B	C	D	E	F	G	H	I	L	M	N	O
1	86	02	20	62 82	22	06	60	3	24	26	84	9

P	Q	R	S	T	U	Z	ET	CON	NON	CHE	Ø
66	68	28	42	80	04 40	88	08	64	00	44	5 7

Текст “CHET CON” может быть зашифрован как 4480564 или 026008702984

Достоинства шифра:

Шифром Ардженти легко как зашифровать текст, так и расшифровать

- Неоднозначность длины и шифрования усложняет процесс расшифровки неприятелем
- Отсутствие ключа

Недостатки шифра:

Шифр не является очень сложным, для расшифровки достаточно иметь

- таблицу алфавита