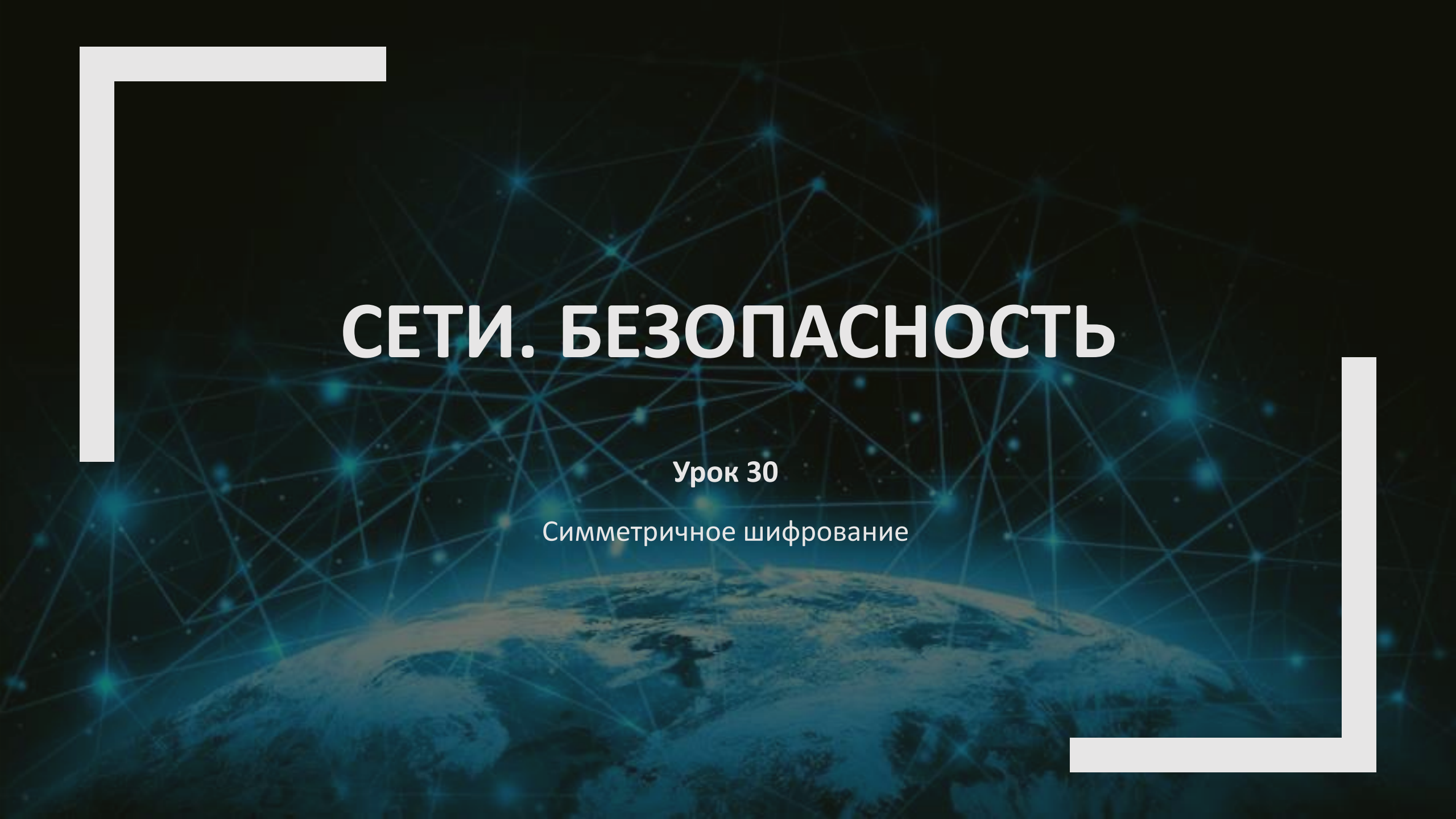
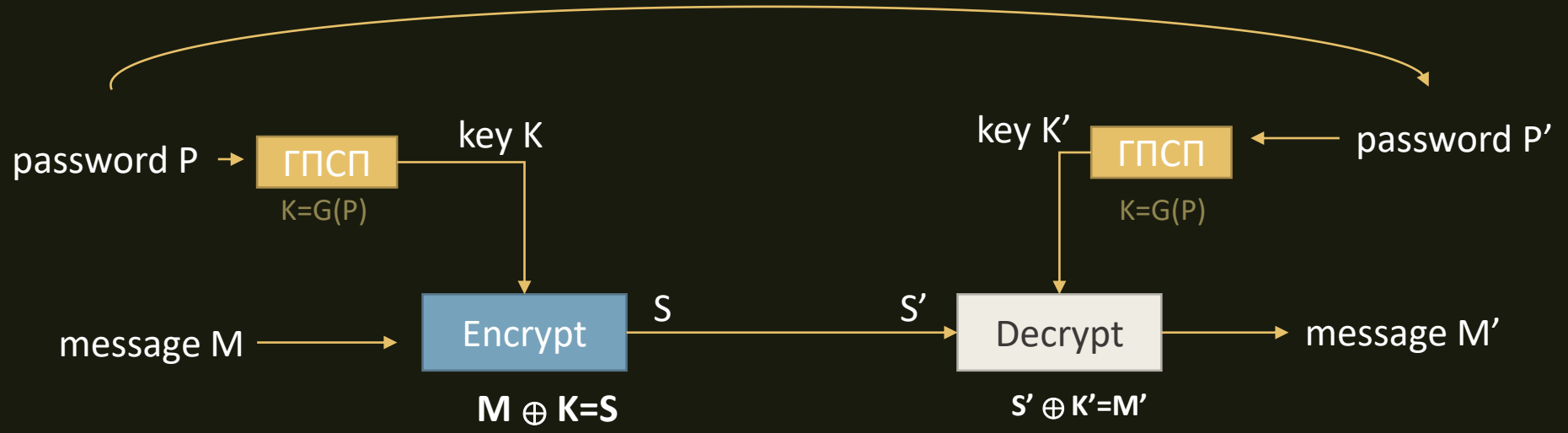


СЕТИ. БЕЗОПАСНОСТЬ

Урок 30

Симметричное шифрование

Полная схема симметричного шифрования



Симметричное шифрование

Функционал

- Однозначность результата шифрования
- Ключ, как элемент алгоритма шифрования

Качество

- Сильная зависимость результата от входных данных
- Непредсказуемость результата
- Длина ключа равна длине сообщения

Стойкость

- Необратимость без ключа
- Стойкость к коллизиям первого рода: невозможно подобрать сообщение или пароль под известный результат
- Стойкость к коллизиям второго рода: невозможно подобрать пару сообщений или паролей с одинаковым результатом
- Стойкость алгоритма тождественна секретности ключа

ГПСП

Функционал

- Однозначность результата
- Неограниченная длина ответа

Качество

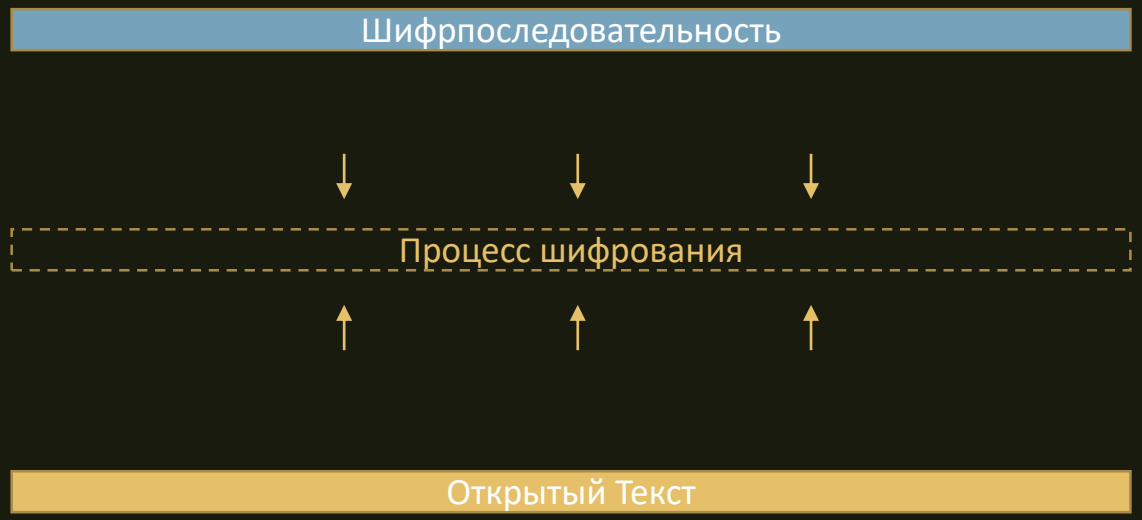
- Сильная зависимость результата от входных данных
- Непредсказуемость результата

Стойкость

- Необратимость
- Стойкость к коллизиям первого рода: невозможно подобрать сообщение или пароль под известный результат
- Стойкость к коллизиям второго рода: невозможно подобрать пару сообщений или паролей с одинаковым результатом

Как оно работает

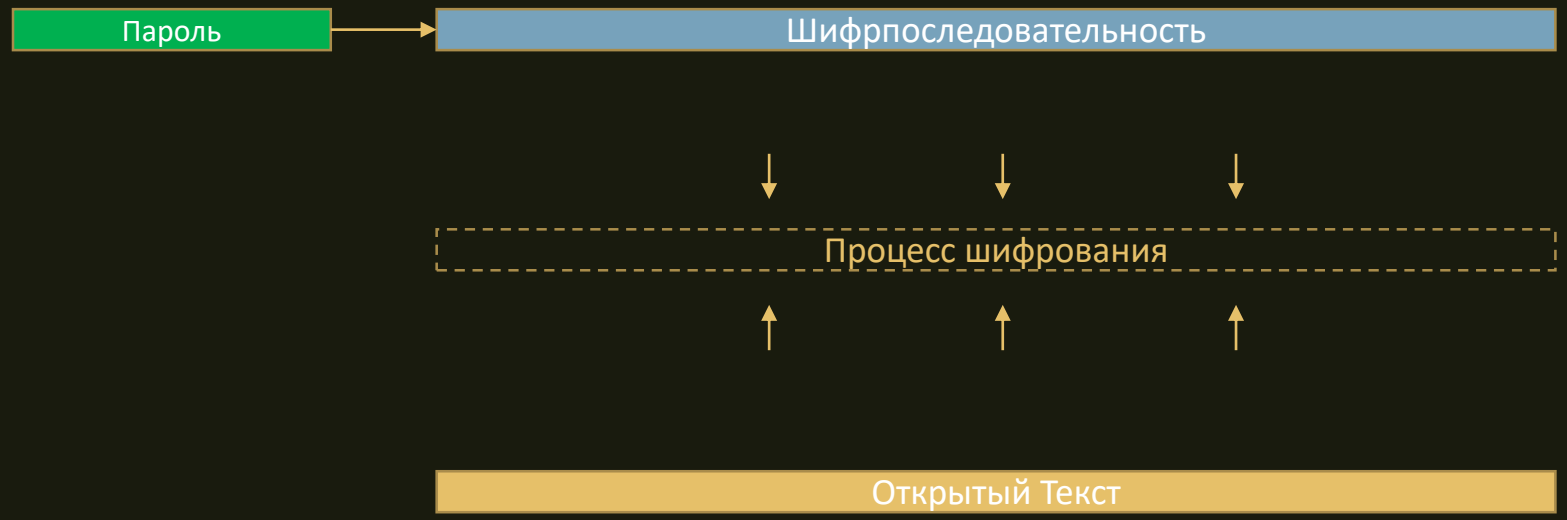
Процесс шифрования



Методики

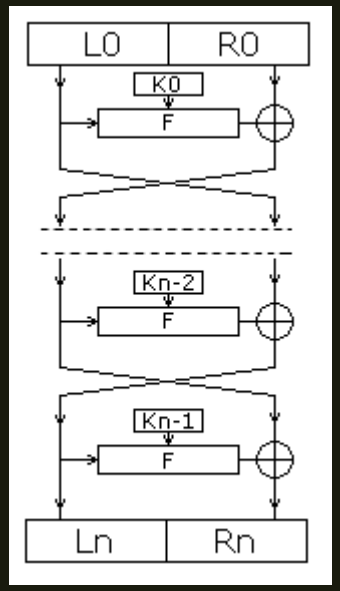
- Гаммирование
  - позволяет реализовать сильное влияние внешних данных
- Перестановки
  - позволяет реализовать взаимное влияние соседних данных
- Замена
  - позволяет скрыть статистические особенности

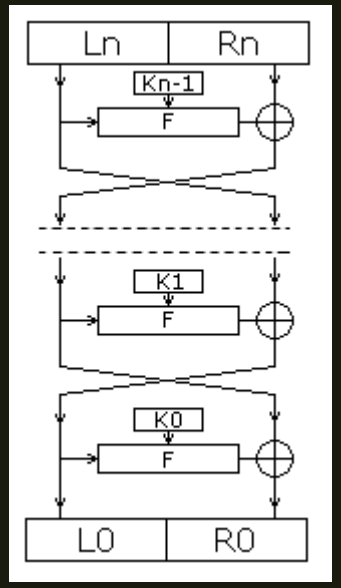
Генерация ключа



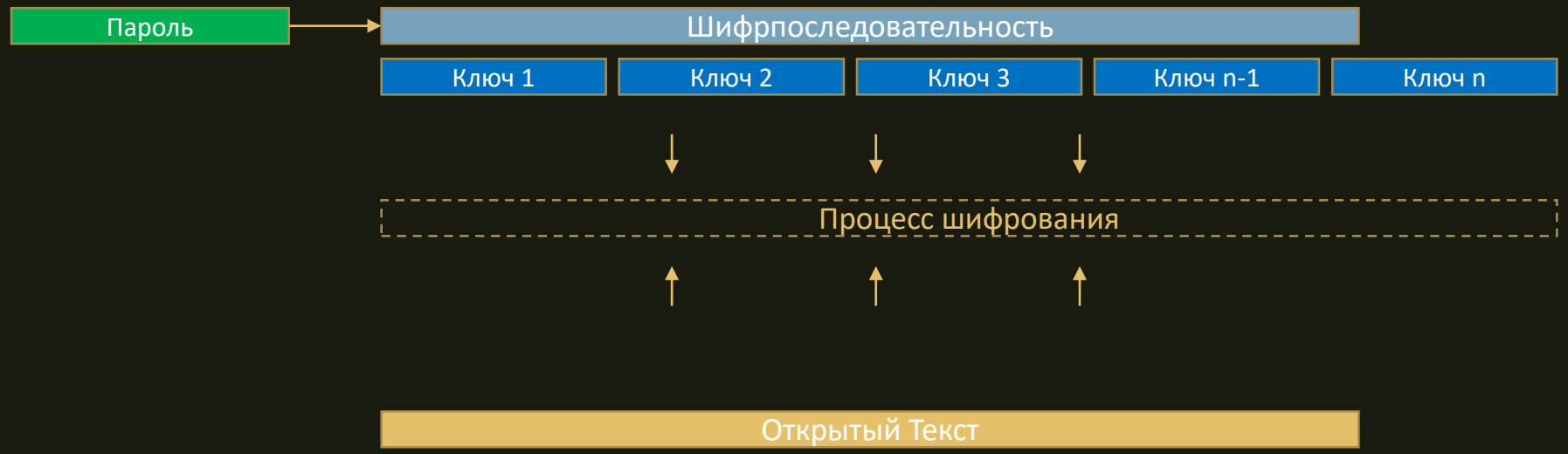
Сеть Фейстеля

- На вход каждой ячейки поступают данные и ключ.
- На выходе каждой ячейки получают изменённые данные и изменённый ключ.
- Все ячейки однотипны
- Ключ выбирается в зависимости от алгоритма шифрования/расшифрования и меняется при переходе от одной ячейки к другой.
- При шифровании и расшифровании выполняются одни и те же операции; отличается только порядок ключей.
- Ввиду простоты операций сеть Фейстеля легко реализовать как программно, так и аппаратно.
- Большинство современных блочных шифров (DES, RC2, RC5, RC6, Blowfish, FEAL, CAST-128, TEA, XTEA, XXTEA и др.) используют сеть Фейстеля в качестве основы.

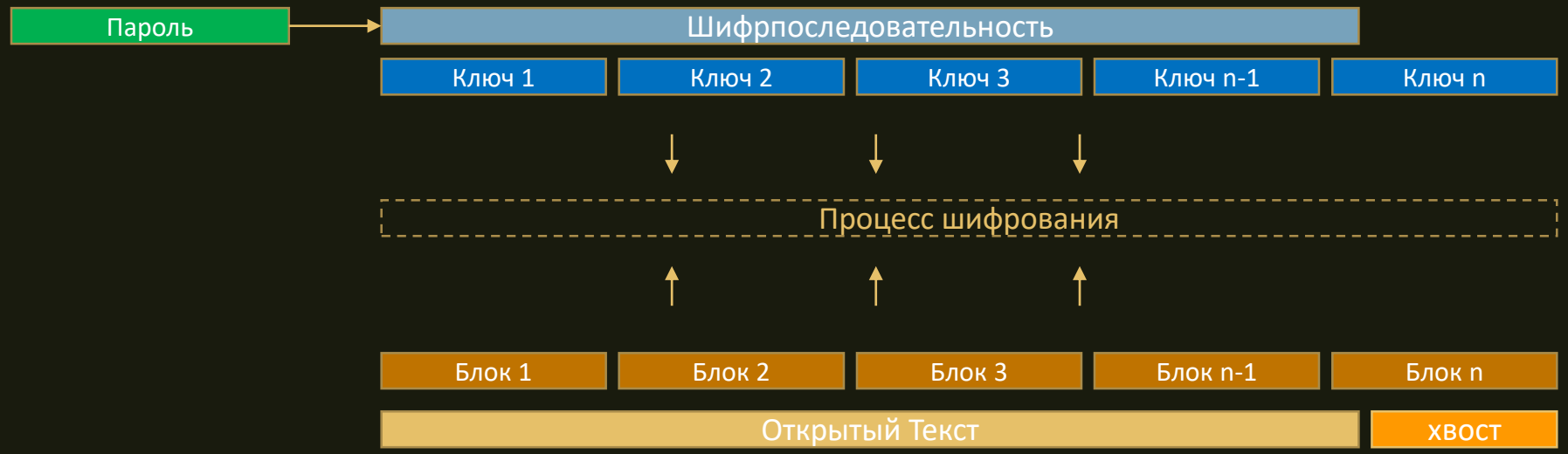




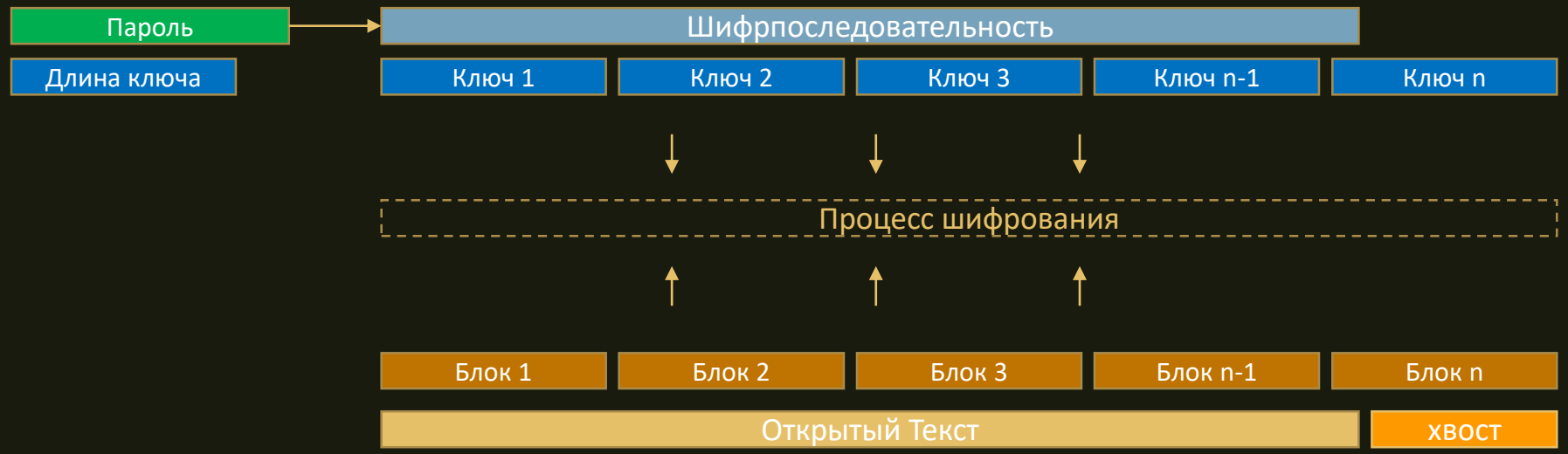
Сеансовые ключи



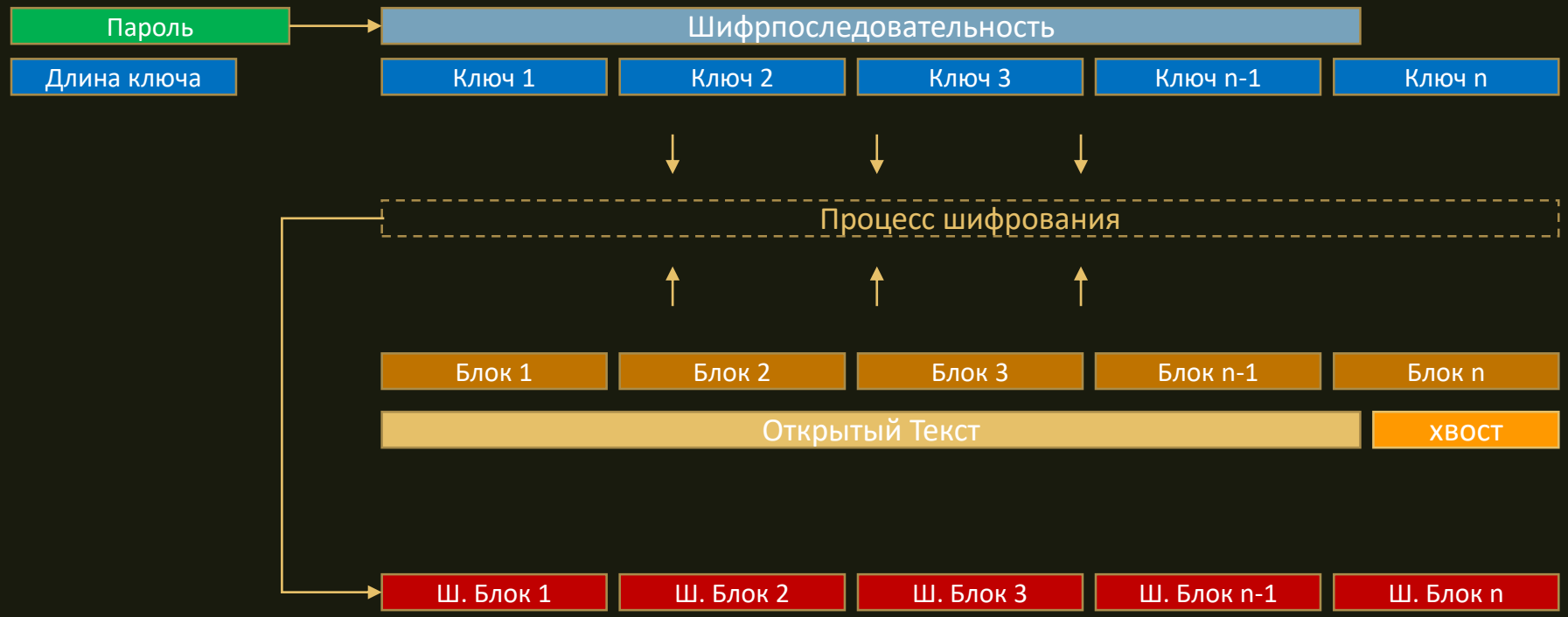
Выравнивание данных



Сжатие ключа

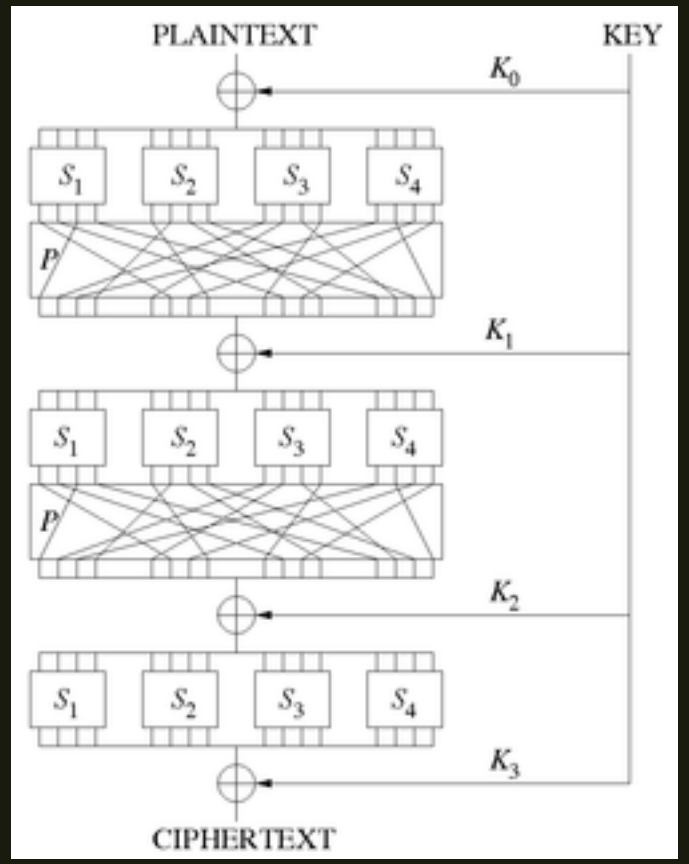


Раунд


Пароль
Шифрпоследовательность
Длина ключа
Ключ 1
Ключ 2
Ключ 3
Ключ n-1
Ключ n
Процесс шифрования
Блок 1
Блок 2
Блок 3
Блок n-1
Блок n
Открытый Текст
хвост
Ш. Блок 1
Ш. Блок 2
Ш. Блок 3
Ш. Блок n-1
Ш. Блок n

Подстановочно-перестановочная сеть

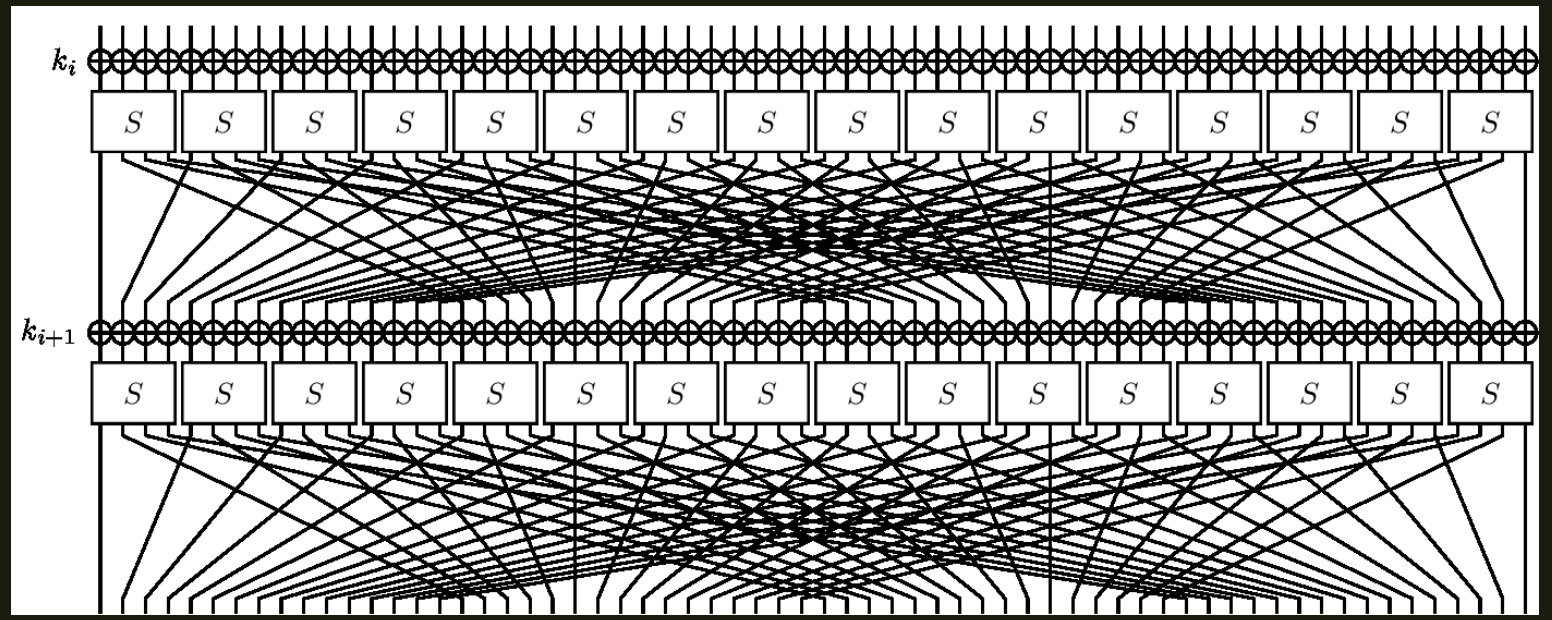
- Шифр на основе SP-сети получает на вход блок и ключ и совершает несколько чередующихся раундов, состоящих из чередующихся стадий подстановки (англ. substitution stage) и стадий перестановки (англ. permutation stage).
  - Для достижения безопасности достаточно одного S-блока, но такой блок будет требовать большого объёма памяти. Поэтому используются маленькие S-блоки, смешанные с P-блоками.
  - Нелинейная стадия подстановки перемешивает биты ключа с битами открытого текста, создавая конфузию Шеннона.
  - Линейная стадия перестановки распределяет избыточность по всей структуре данных, порождая диффузию.
- S-блок (англ. substitution box or S-box) замещает маленький блок входных бит на другой блок выходных бит.
  - Эта замена должна быть взаимно однозначной, чтобы гарантировать обратимость.
  - Назначение S-блока заключается в нелинейном преобразовании, что препятствует проведению линейного криптоанализа.
  - Одним из свойств S-блока является лавинный эффект, т.е. изменение одного бита на входе приводит к изменению всех бит на выходе.
- P-блок (англ. permutation box or P-box) — перестановка всех бит: блок получает на вход вывод S-блока, меняет местами все биты и подает результат S-блоку следующего раунда.
  - Важным качеством P-блока является возможность распределить вывод одного S-блока между входами как можно больших S-блоков.
- Для каждого раунда используется свой, получаемый из первоначального, ключ. Подобный ключ называется раундовым. Он может быть получен как делением первоначально ключа на равные части, так и каким-либо преобразование всего ключа.

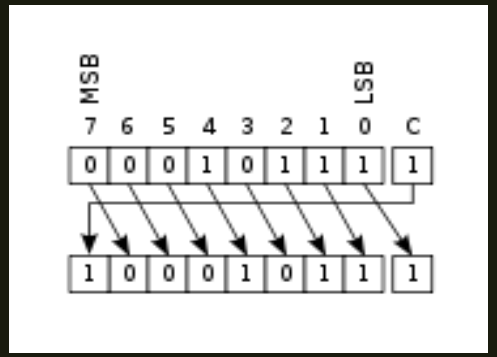


S-блок

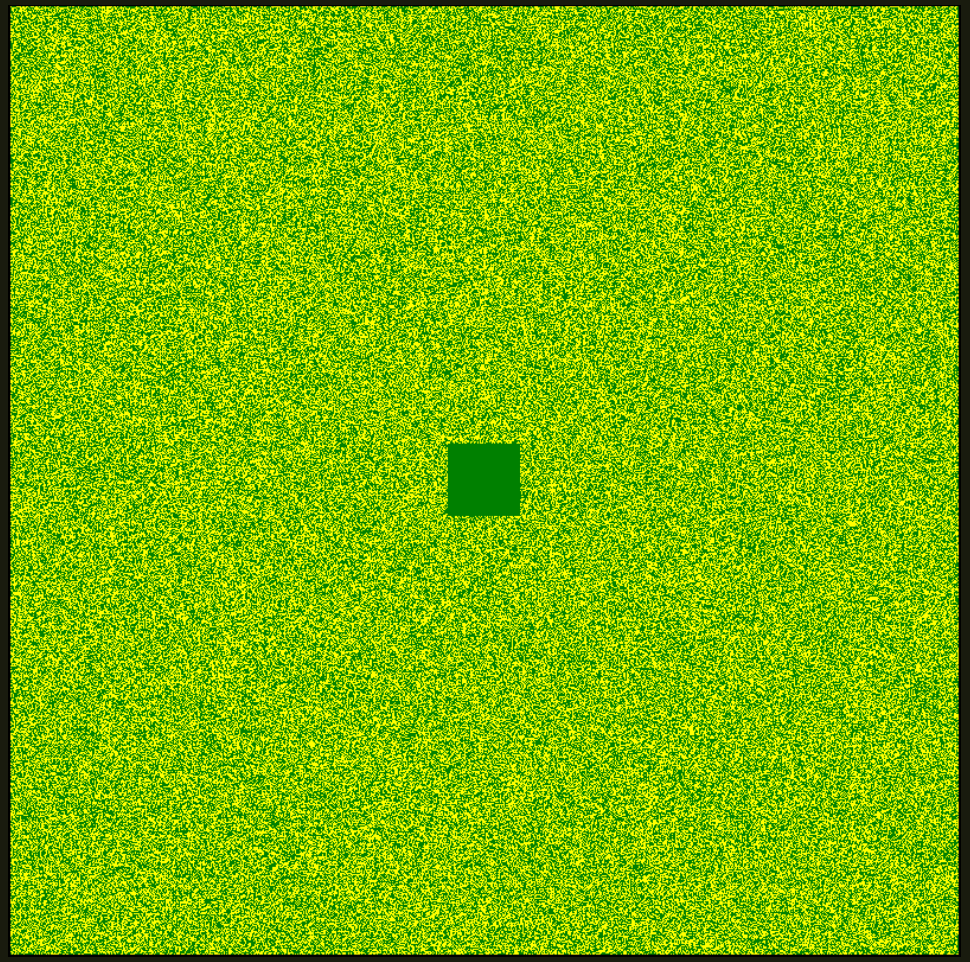
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

P-блок

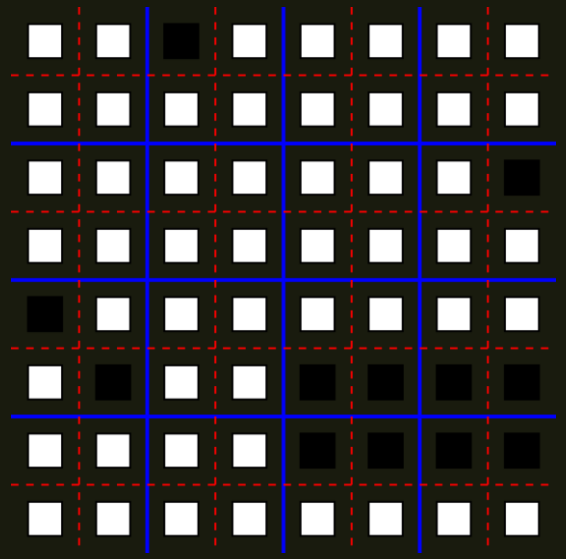




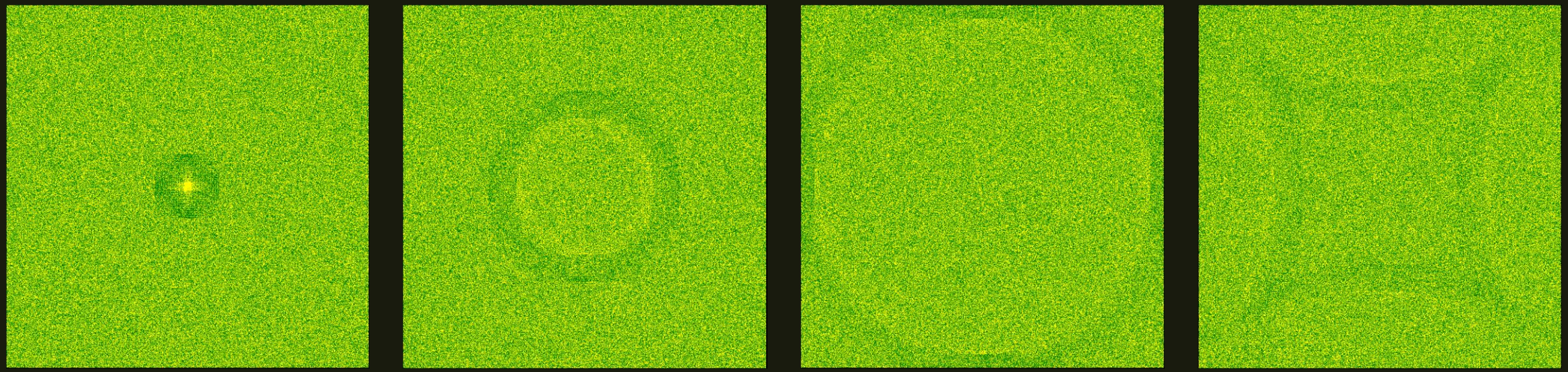
P-блок. Экзотические методики



- Клеточный автомат
- Чередующиеся ячейки 2x2 (окрестность Марголуса)
- Данные 640 кб и Ключ 10 кб (в центре)
- Алгоритм – инверт ячейки 2x2



Распространение хаоса



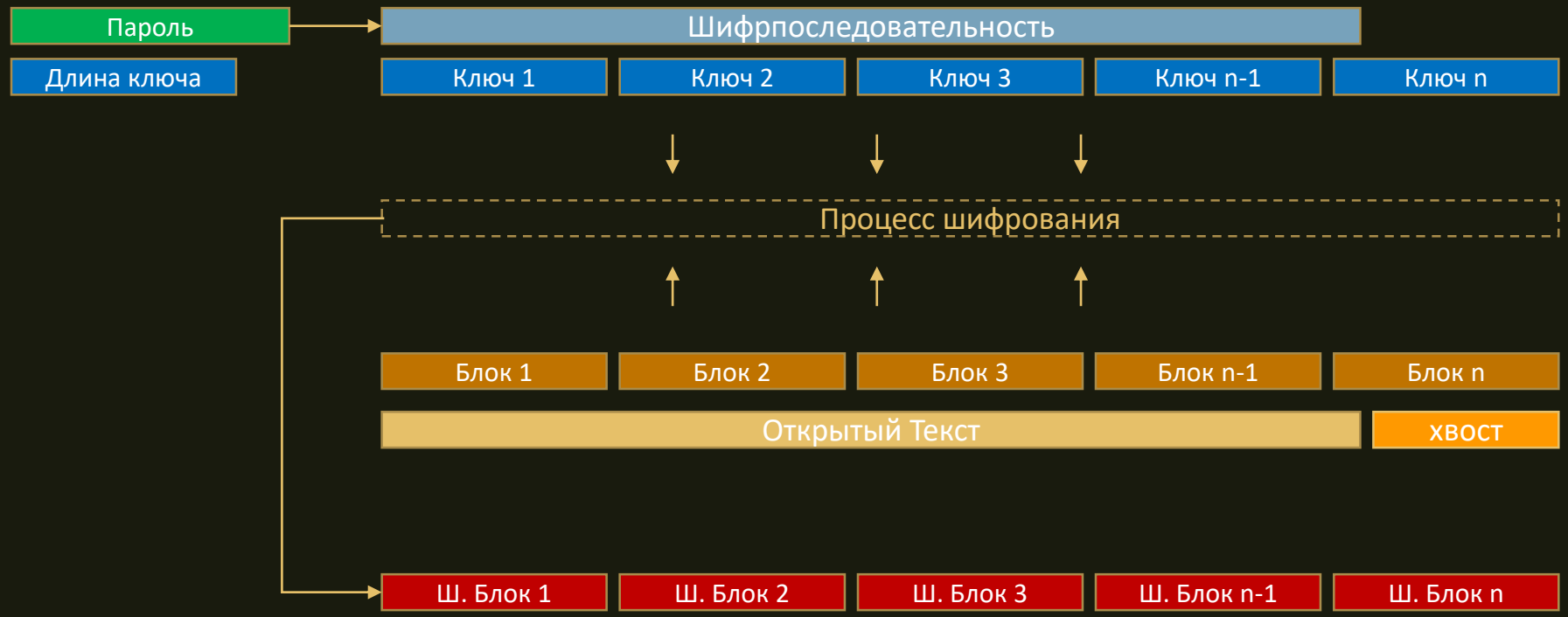
20 раундов

90 раундов

200 раундов

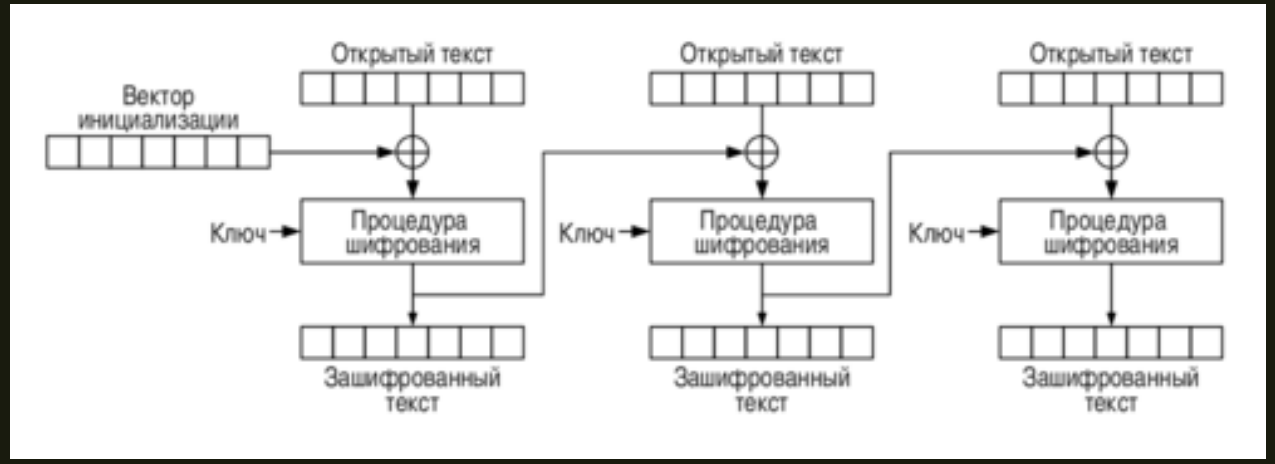
300 раундов

Раунд

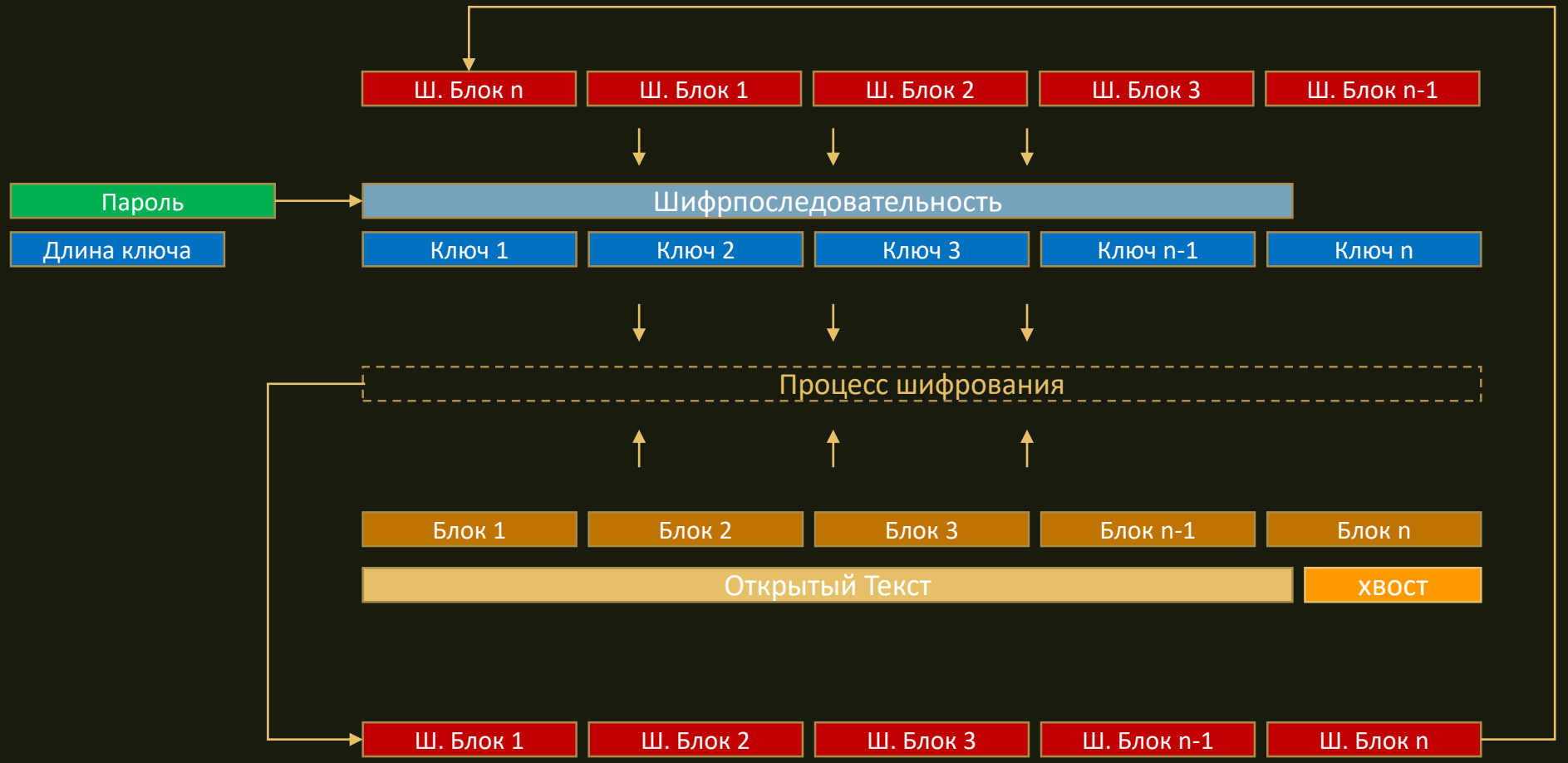

Пароль
Шифрпоследовательность
Длина ключа
Ключ 1
Ключ 2
Ключ 3
Ключ n-1
Ключ n
Процесс шифрования
Блок 1
Блок 2
Блок 3
Блок n-1
Блок n
Открытый Текст
хвост
Ш. Блок 1
Ш. Блок 2
Ш. Блок 3
Ш. Блок n-1
Ш. Блок n

Каскадность результата

- Результат шифрования каждого блока используется для шифрования следующего блока
- Результат последнего блока зависит от результатов всех предыдущих
- Результат первого блока не связан с результатами последующих



Процесс


Ш. Блок n
Ш. Блок 1
Ш. Блок 2
Ш. Блок 3
Ш. Блок n-1
Пароль
Шифрпоследовательность
Длина ключа
Ключ 1
Ключ 2
Ключ 3
Ключ n-1
Ключ n
Процесс шифрования
Блок 1
Блок 2
Блок 3
Блок n-1
Блок n
Открытый Текст
хвост
Ш. Блок 1
Ш. Блок 2
Ш. Блок 3
Ш. Блок n-1
Ш. Блок n

ToDo

- Выравнивание данных
- Сжатие ключа
- Генерация сеансовых ключей
- Блок G (гаммирование)
- Блок P (перестановки)
- Блок S (подстановки)
- Добавление раундовой соли
- Раундовая каскадность

ToDo (min)

- Выравнивание данных
- Сжатие ключа
- Генерация сеансовых ключей
- Блок G (гаммирование)
- Блок P (перестановки)
- Блок S (подстановки)
- Добавление раундовой соли
- Раундовая каскадность