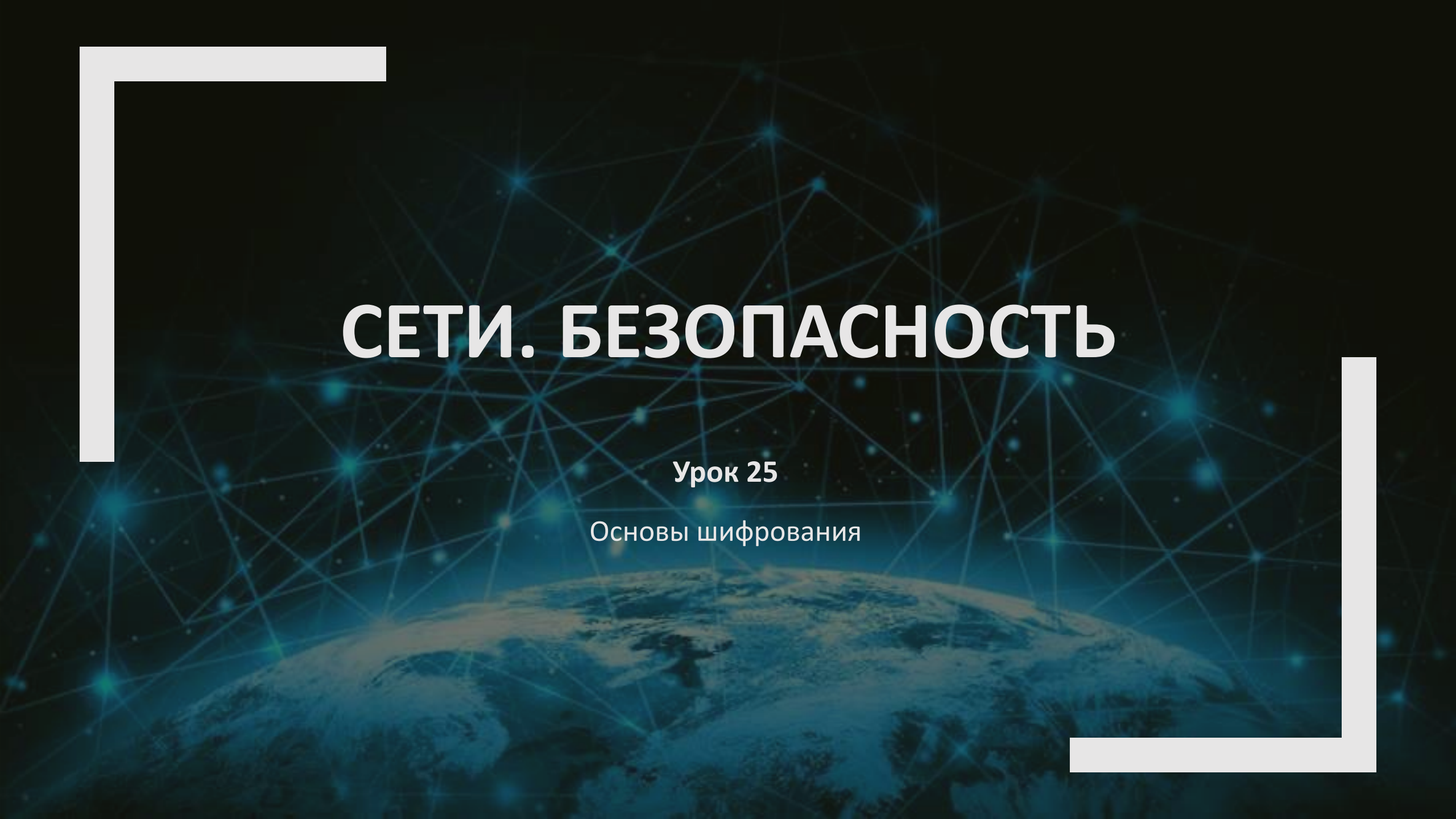


СЕТИ. БЕЗОПАСНОСТЬ

Урок 25

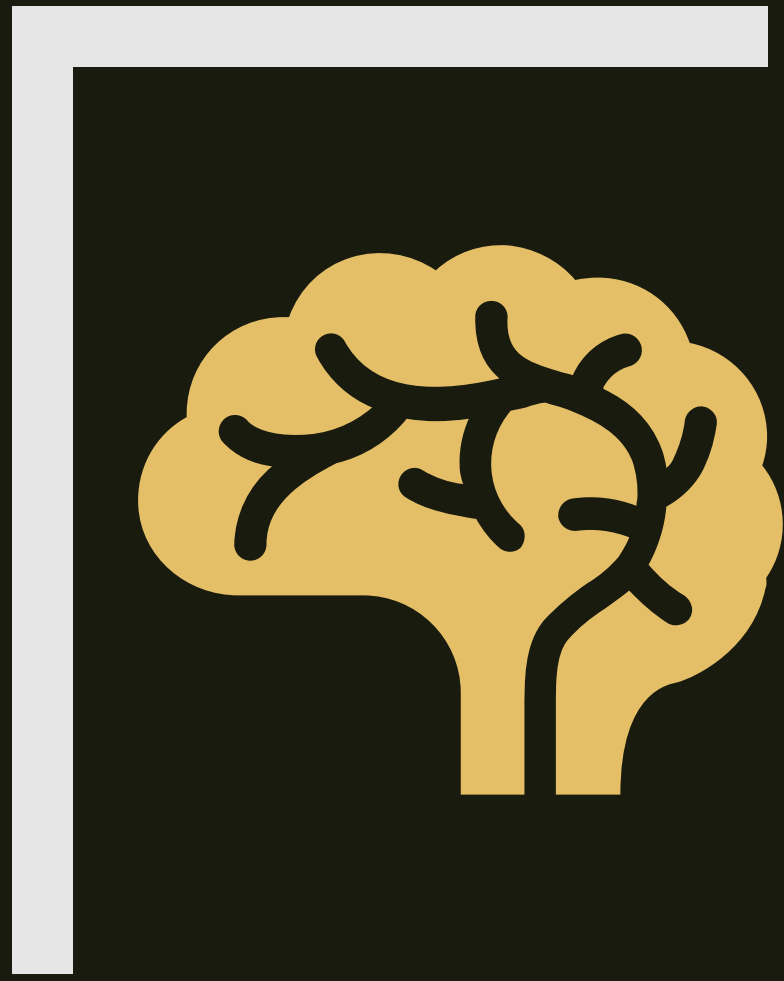
Основы шифрования

Memory line

Кодирование

vs

Шифрование



Шифрование

Шифрование

Шифрование — обратимое преобразование информации в целях сокрытия от неавторизованных лиц…

… с предоставлением, в это же время, **авторизованным** пользователям доступа к ней.

Авторизация

- **Авториза́ция** — предоставление определённому лицу или группе лиц прав на выполнение определённых действий; а также процесс проверки (подтверждения) данных прав при попытке выполнения этих действий.

- **Аутентифика́ция** — процедура проверки подлинности данных, например:
  - проверка подлинности пользователя путём сравнения введённого им пароля с паролем, сохранённым в базе данных пользователей;
  - подтверждение подлинности электронного письма путём проверки цифровой подписи письма по открытому ключу отправителя;
  - проверка контрольной суммы файла на соответствие сумме, заявленной автором этого файла.

***шифрование

- Шифрование – закрытие информации
- Расшифрование – открытие информации авторизованным лицом
- Дешифрование – открытие информации **НЕ**авторизованным лицом

Шифрование

С помощью шифрования обеспечиваются три состояния безопасности информации:

- Конфиденциальность.
  - Шифрование используется для скрытия информации от неавторизованных пользователей при передаче или при хранении.
- Целостность.
  - Шифрование используется для предотвращения изменения информации при передаче или хранении.
- Идентифицируемость.
  - Шифрование используется для аутентификации источника информации и **предотвращения отказа отправителя** информации от того факта, что данные были отправлены именно им.

Разновидности

- Блочные шифры
  - Обрабатывают информацию блоками определённой длины (обычно 64, 128 бит), применяя к блоку ключ в установленном порядке, как правило, несколькими циклами перемешивания и подстановки, называемыми раундами.

- Поточные шифры
  - В которых шифрование проводится над каждым битом либо байтом исходного текста с использованием гаммирования.

Разновидности

- Открытый/Закрытый ?

Разновидности

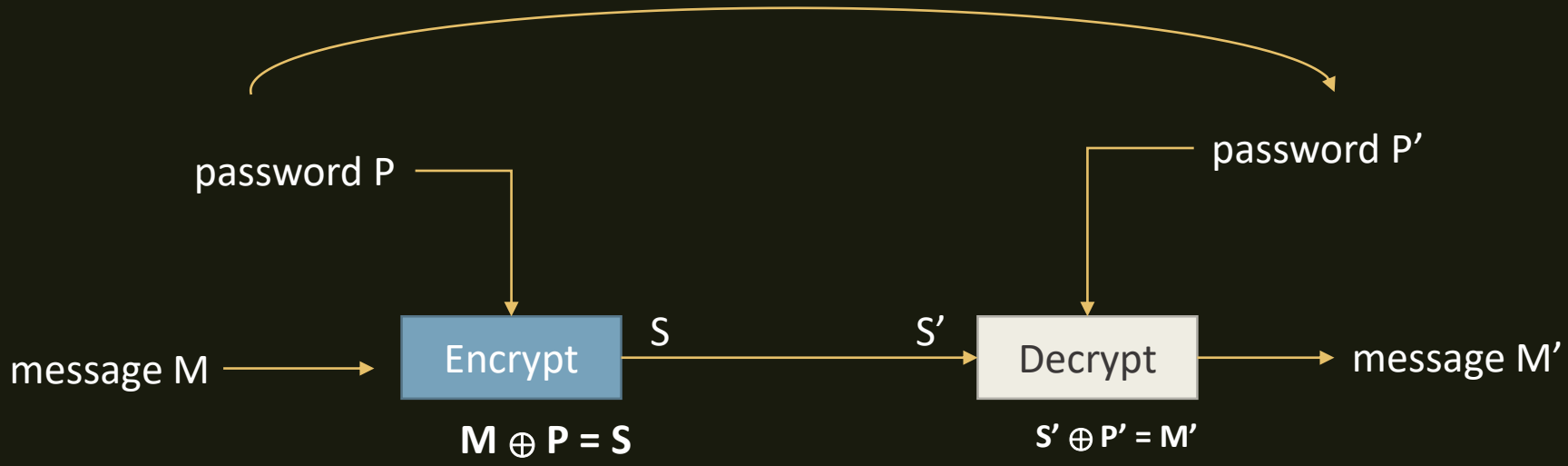
- Открытый/Закрытый ?

Принцип Керкгоффса : Враг знает систему

С.Ш. и А.Ш.

- Симметричное
  - Простое
  - Быстрое
  - Эффективное
- Асимметричное
  - Архисложное
  - Долгое
  - «Мистическое»

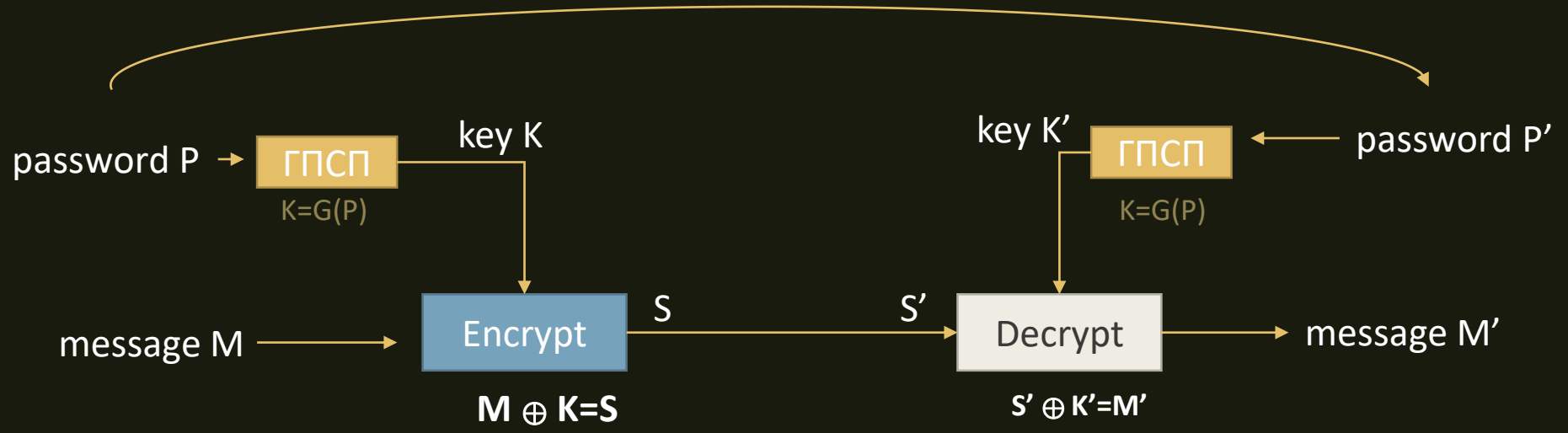
Полная схема симметричного шифрования



Основные требования

- 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

Полная схема симметричного шифрования



Мировые стандарты

Блочные шифрыAES (англ. Advanced Encryption Standard) - американский стандарт шифрования

- ГОСТ 28147-89 советский и российский стандарт шифрования, также является стандартом СНГ
- DES/AES (англ. Data Encryption Standard) - стандарт шифрования данных в США
- 3DES (Triple-DES, тройной DES)
- RC2 (Шифр Ривеста (Rivest Cipher или Ron’s Cipher))
- RC5
- Blowfish
- Twofish
- NUSH
- IDEA (International Data Encryption Algorithm, международный алгоритм шифрования данных)
- CAST (по инициалам разработчиков Carlisle Adams и Stafford Tavares)
- CRAB
- 3-WAY
- Khufu и Khafre
- Kuznechik

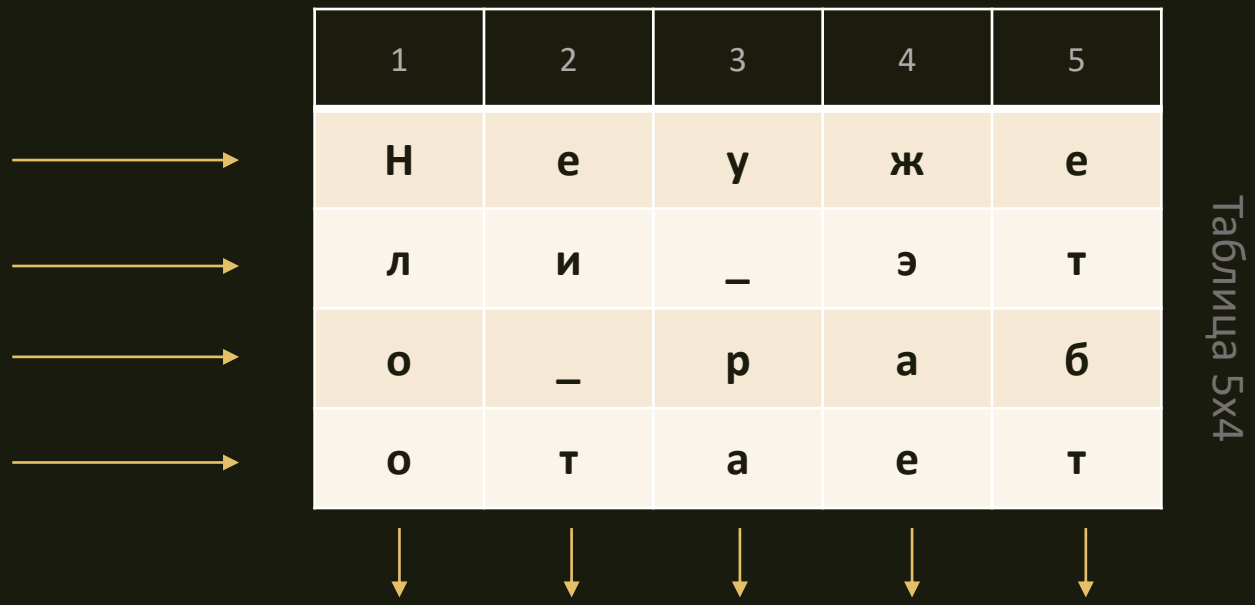
Потоковые шифры

- RC4 (алгоритм шифрования с ключом переменной длины)
- SEAL (Software Efficient Algorithm, программно-эффективный алгоритм)
- WAKE (World Auto Key Encryption algorithm, всемирный алгоритм шифрования на автоматическом ключе)

Шифрование. Начало практики

Табличная перестановка

Неужели это работает (20 символов)



Нлооеи ту ражэаеетбт

Лексиграфический ключ

Неужели это работает

(20 символов)

А	К	У	Л	А
Н	е	у	ж	е
л	и	_	э	т
о	_	р	а	б
о	т	а	е	т

Таблица 5x4

Лексиграфический ключ

Неужели это работает

(20 символов)

А	К	У	Л	А
1	3	5	4	2
Н	е	у	ж	е
л	и	_	э	т
о	_	р	а	б
о	т	а	е	т

Таблица 5x4

Табличная перестановка

Неужели это работает

(20 символов)

А	К	У	Л	А
1	3	5	4	2
Н	е	у	ж	е
л	и	_	э	т
о	_	р	а	б
о	т	а	е	т

Таблица 5x4

Нлоо

Табличная перестановка

Неужели это работает

(20 символов)

А	К	У	Л	А
1	3	5	4	2
Н	е	у	ж	е
л	и	_	э	т
о	_	р	а	б
о	т	а	е	т

Таблица 5x4

Нлооетбт

Табличная перестановка

Неужели это работает

(20 символов)

А	К	У	Л	А
1	3	5	4	2
Н	е	у	ж	е
л	и	_	э	т
о	_	р	а	б
о	т	а	е	т

Таблица 5x4

Нлооетбтеи т

Табличная перестановка

Неужели это работает

(20 символов)

А	К	У	Л	А
1	3	5	4	2
Н	е	у	ж	е
л	и	_	э	т
о	_	р	а	б
о	т	а	е	т

Таблица 5x4

Нлооетбтеи тжэае

Табличная перестановка

Неужели это работает

(20 символов)

А	К	У	Л	А
1	3	5	4	2
Н	е	у	ж	е
л	и	_	э	т
о	_	р	а	б
о	т	а	е	т

Таблица 5x4

Нлооетбтеи тжэаеу ра

Табличная перестановка

Неужели это работает

(20 символов)

А	К	У	Л	А
1	3	5	4	2
Н	е	у	ж	е
л	и	_	э	т
о	_	р	а	б
о	т	а	е	т

Таблица 5x4

Нлооетбтеи тжэаеу ра

Табличная перестановка

Чыосеаповно!рч тзйр!

20 букв. Пароль: АГАМА

Табличная перестановка

Чыосеаповно!рч тзйр!

А	Г	А	М	А

Табличная перестановка

Чыосеаповно!рч тзйр!

А	Г	А	М	А
1		2		3

Табличная перестановка

Чыосеаповно!рч тзйр!

А	Г	А	М	А
1	4	2	5	3

Табличная перестановка

Чыосеаповно!рч тзйр!

А	Г	А	М	А
1	4	2	5	3
Ч				
ы				
о				
с				

Табличная перестановка

Чыосеаповно!рч тзйр!

А	Г	А	М	А
1	4	2	5	3
Ч		е		
ы		а		
о		п		
с		о		

Табличная перестановка

Чыосеапо**вно!**рч тзйр!

А	Г	А	М	А
1	4	2	5	3
Ч		**е**		**в**
ы		**а**		**н**
о		**п**		**о**
с		**о**		**!**

Табличная перестановка

Чыосеаповно!рч тзйр!

А	Г	А	М	А
1	4	2	5	3
Ч	р	е		в
ы	ч	а		н
о		п		о
с	т	о		!

Табличная перестановка

Чыосеаповно!рч тзйр!

А	Г	А	М	А
1	4	2	5	3
Ч	р	е	з	в
ы	ч	а	й	н
о		п	р	о
с	т	о	!	!

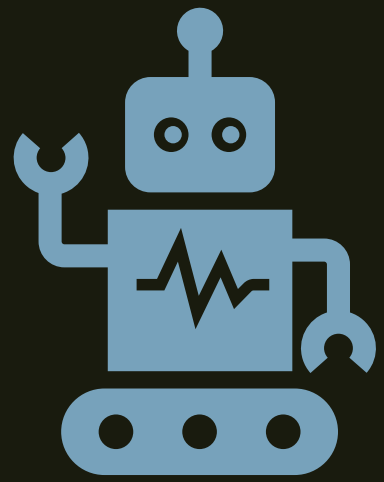
Табличная перестановка

Чыосеаповно!рч тзйр!

А	Г	А	М	А
1	4	2	5	3
Ч	р	е	з	в
ы	ч	а	й	н
о		п	р	о
с	т	о	!	!

Чрезвычайно просто!!

Практика



Практика

Задачи!! …. Вас ждут задачи!!!