ЗАЩИТА ИНФОРМАЦИИ

Воронцова Татьяна [Дмитриевна]

Ведущий программист УИЛ функциональной безопасности космических аппаратов и систем
Окончила специалитет «Компьютерная безопасность» департамента Прикладная математика факультета МИЭМ им А.Н. Тихонова НИУ ВШЭ

id191493257

07.10 – 1 Безопасность информации. Математический аппарат

09.10 – 2 Теория кодирования

13.10 – 3 Криптография

15.10 – 4 Шифрование

19.10 – 5 Экзамен

ПЛАН ЛЕКЦИЙ

4 учебных занятия, по 3 часа:

- Посещаемость (минимум половина занятий)
- Промежуточный контроль (3 теста)
- Теория
- Практика
- Домашняя работа

Экзамен (по желанию) 19 октября.

ТЕСТ ПО МАТЕРИАЛАМ ТРЕТЬЕГО УРОКА

Начало: 15.30

Окончание: 15.50

Результаты будут объявлены после перерыва

https://forms.gle/EiA9sGLtg29WuDGY9

ШИФРОВАНИЕ

Защита информации. Лекция 4

СИММЕТРИЧНОЕ ШИФРОВАНИЕ

Идея: зашифровываем и расшифровываем одним ключом

Алгоритм:

- Генерируем ключ k: А и Б знают, Е – нет;
- А шифрует сообщение на ключе k, отправляет шифртекст по открытому каналу;
- Б расшифровывает полученное на ключе k, получает открытый текст.

Вопрос: как скрыть ключ от Евы?

- Закрытый канал
- Сеансовый ключ

Асимметричное шифрование

Идея: зашифровываем и расшифровываем разными ключами, причем они связаны между собой, но зная открытый слишком трудно вычислить закрытый

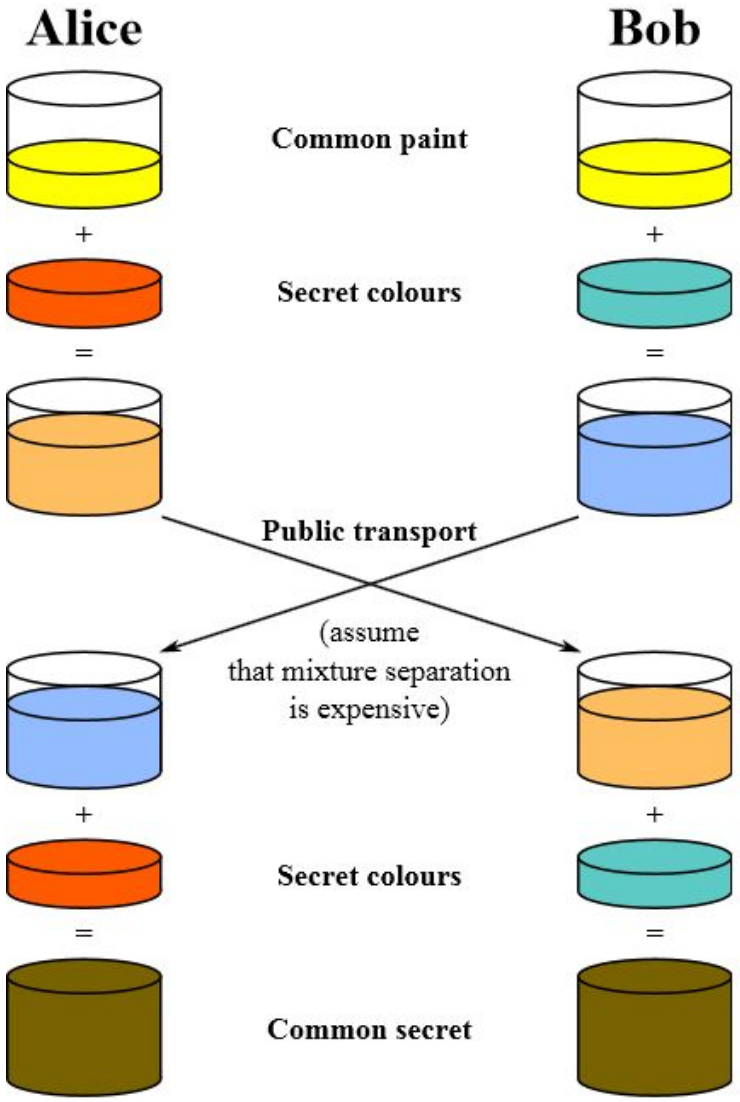
Алгоритм:

- Б генерирует пару ключей (e,d) – открытый и закрытый, открытый публикуется в открытом доступе;
- А хочет написать сообщение Б, берет его открытый ключ e и шифрует сообщение на ключе e, отправляет шифртекст по открытому каналу;
- Ева не знает d, поэтому не сможет прочитать сообщение;
- Б расшифровывает полученное на ключе d, получает открытый текст.

Вопрос: Что может сделать Ева?

ШИФРОВАНИЕ СЕАНСОВОГО КЛЮЧА

ПРОТОКОЛ ДИФФИ-ХЕЛЛМАНА



- Открытый ключ:
  - p – простое (модуль)
  - g – примитивный корень

$$\begin{cases} g^{\phi(p)} \equiv 1 \bmod p \\ g^{l} \not\equiv 1 \bmod p, \end{cases} \forall l \neq \phi(m)$$

Модуль поля	Порождающий	Модуль поля	Порождающий	Модуль поля	Порождающий
3	2	59	2	131	2
5	2	61	2	137	3
7	3	67	2	139	2
11	2	71	7	149	2
13	2	73	5	151	6
17	3	79	3	157	5
19	2	83	2	163	2
23	5	89	3	167	5
29	2	97	5	173	2
31	3	101	2	179	2
37	2	103	5	181	2
41	6	107	2	191	19
43	3	109	6	193	5
47	5	113	3	197	2
53	2	127	3	199	3

Основные понятия лекции

- Симметричное шифрование
- Асимметричное шифрование
- ЭЦП
- Сеансовый ключ
- Протокол Диффи-Хеллмана
- Хэш-функция