Джентльменский набор криптографа

1. Основные понятия и обозначения

- **Криптосистема** $= (\mathcal{M}_{\text{ОТ}}, \mathcal{C}_{\text{КГ}}, \mathcal{K}_{\text{ключей}}, E_{\text{шифр}}, D_{\text{расшифр}})$:
  - $\mathcal{M}_{\text{ОТ}}$ — множество открытых текстов (plain text).
  - $\mathcal{C}_{\text{КГ}}$ — множество криптограмм (cipher text).
  - $\mathcal{K}_{\text{ключей}}$ — множество ключей.
  - $E_{\text{шифр}}$ — функция шифрования.
  - $D_{\text{расшифр}}$ — функция расшифровки.
- **Принцип Керкгоффса**: безопасность криптосистемы должна зависеть только от секретности ключа, а не алгоритма.
- **Совершенная криптосистема**: взаимная информация между открытым текстом и криптограммой равна нулю, т.е. знание шифротекста не даёт информации о тексте.

2. Классические шифры (исторические)

- **Шифр Цезаря**: сдвиг каждой буквы алфавита на фиксированное число n.
- **Шифр Августа**: частный случай шифра Цезаря при $n = 1$.
- **Шифр подстановки (ШПЗ)**: каждой букве ставится в соответствие другая, создавая биекцию.
- **Шифр перестановки (ШП)**: меняется порядок букв в тексте.

- **Квадрат Полибия**: таблица 5×5, каждая буква кодируется координатами строки и столбца.
- **Сцитала**: шифр в виде ленты, наматываемой на цилиндр. Расшифровка возможна только при правильном диаметре.
- **Диск Энея**: устройство с буквами и ниткой. Прототип механических шифраторов.
- **Линейка Энея**: линейная реализация идеи диска Энея.
- **Диск Альберти**: на внешнем круге буквы, на внутреннем — цифры; внутренний диск вращается для создания ключей.
- **ШМЗ**: ключ сопоставляет два алфавита (например, латиницу и кириллицу).
- **Миланский шифр (дадая)**: нарушает частотный анализ — редким буквам соответствует много символов, частым — один.
- **Таблица Тритемия**: последовательное применение шифров Цезаря по таблице.
- **Шифр Беллазо**: таблица Тритемия, в которой выбор строки определяется повторяющимся паролем.
- **Шифр Виженера**: каждая буква ОТ шифруется своей буквой ключа $K = k_1 k_2 \dots k_m$, ключ повторяется.
- **Шифр Вернама**: как у Виженера, но ключ такой же длины, как и текст $\Rightarrow$ совершенная защита.
- **Решётка Кардано**: лист с дырками, накладываемый на текст, поворачивается для получения всего сообщения.
- **Джефферсонов цилиндр**: набор вращающихся дисков с алфавитами.
- **Уитстона–Плейфера**: шифрование биграмм с циклическим сдвигом.
- **Устройство Уодстворта**: вложенные шестерёнки для создания сложных замен.

- **Хагелин (B-21)**: электромеханическое устройство с дисками разного диаметра.
- **Шифр Хилла**: $C = K \cdot M$, где K — матрица-ключ. Уязвим из-за линейности.
- **Шербиус**: основа Enigma (электромеханическая система).

3. Атаки на шифры

1. **Ciphertext-only**: Ева знает только зашифрованный текст.
2. **Known-plaintext**: Ева знает часть открытого текста и соответствующую криптограмму.
3. **Chosen-plaintext**: Ева может выбирать тексты и получать соответствующие шифротексты.
4. **Chosen-ciphertext**: Ева может выбирать криптограммы и получать их расшифровку.

4. Теория информации

- **Энтропия (H)** — мера неопределённости случайной величины:

$$H(X) = -\sum p_i \log_2 p_i$$

- **Информация события**:

$$I(p) = -\log_2 p$$

- **Условная информация**:

$$I(a|b) = -\log_2 P(a|b)$$

- **Индекс совпадений (IC)** — вероятность совпадения случайно выбранных двух символов.

- **Метод Фридмана**: оценка длины ключа по статистике совпадений.
- **Избыточность языка** — часть информации, не несущая смысла (например, буква "о"в русском).
- **Стационарная модель ОТ** — вероятности символов не зависят от их позиции в тексте.
- **Энтропия языка** — предельная энтропия на символ при бесконечной длине текста.

5. Расстояния и искажения

- **Расстояние Хэмминга**: число позиций, в которых строки отличаются.
- **Sub(w)**: множество всех слов, отличающихся от w на одинаковое число символов.
- **Теорема Маркова**: функция шифрования сохраняет расстояние Хэмминга (является изометрией).
- **Расстояние единственности**: минимальная длина текста, начиная с которой его можно расшифровать однозначно.

6. Блочные шифры и преобразования

- **Блочные шифры**: шифруются блоки символов (обычно по 64 бита и более).
- **Рассеивающие преобразования**: усложняют структуру текста, воздействуют на малые участки.
- **Перемешивающие преобразования**: простые, воздействуют на весь блок.
- **Конструкция Фейстеля**: текст делится пополам, к одной половине применяется функция от другой, затем половины меняются местами. Основа DES.

7. Атаки типа подмены и имитации

- **Атака подмены**: Ева заменяет отправленное сообщение другим.
- **Атака имитации**: Ева отправляет сообщение от лица Алисы, хотя та ничего не отправляла.

8. Дополнительно

- **Теорема Глухова**: описывает все возможные ШПЗ, не допускающие искажений типа "пропуск".
- **Эндоморфная КС**: $|\mathcal{M}| \leq |\mathcal{C}|$ — множество сообщений не больше множества шифров.
- **Теорема Шеннона 1**: если энтропия близка к информации на символ, то сообщение типичное.
- **Теорема о 9-ти точках**: *осталась как загадка.* Часто используется в шутливом контексте.