Существует **четыре** основных типа криптоаналитического вскрытия . Для каждого из них предполагается, что криптоана-литик обладает всей полнотой знания об используемом алгоритме шифрования :

.**Вскрытие с использованием только шифротекста**. У крипто-аналитика есть шифротексты нескольких сообщений, зашифрованных одним и тем же алгоритмом шифрования . Задача криптоаналитика состоит в раскрытии открытого текста как можно большего числа сообщений или, что лучше, получении ключа (ключей), использованного для шифрования сообщений, для дешифрировании других сообщений, зашифрованных теми же ключами.

Дано: $C_1=E_k(P_1)$, $C_2=E_k(P_2)$, . . . $Ci=E_k(P_i)$

Получить: Либо P_1, P_2, . . . Pi; k; либо алгоритм, как получать P_{i+1} из $C_{i+1}=E_k(P_{i+1})$

2. **Вскрытие с использованием открытого текста**. У крипто-аналитика есть доступ не только к шифротекстам нескольких сообщений, но и к открытому тексту этих сообщений . Его задача состоит в получении ключа (или ключей), использованного для шифрования сообщений, для дешифрировании других сообщений, зашифрованных тем же ключом (ключами).

Дано: P_1, $C_1=E_k(P_1)$, P_2, $C_2=E_k(P_2)$, . . . P_i, $C_i=E_k(P_i)$ Получить: либо k; либо алгоритм, как получать

P_{i+1} из $C_{i+1}=E_k(P_{i+1})$

3. **Вскрытие с использованием выбранного открытого текста**.

У криптоаналитика не только есть доступ к шифротекстам и открытым текстам нескольких сообщений, но и возможность выбирать открытый текст для шифрования. Это предоставляет больше вариантов чем вскрытие с использованием открытого текста, так как криптоаналитик может выбирать шифруемые блоки открытого текста, что может дать больше информации о ключе. Его задача состоит в получении ключа (или ключей), использованного для шифрования сообщений, или алгоритма, позволяющего дешифрировать новые сообщения, зашифрованные тем же ключом (или ключами).

Дано: P_1, $C_1=E_k(P_1)$, P_2, $C_2=E_k(P_2)$, . . . P i, $C_i=E_k(P_i)$ где криптоаналитик может выбирать P_1, P_2, . . . P_i

Получить: либо k; либо алгоритм, как получать

P_{i+1} из $C_{i+1}=E_k(P_{i+1})$

4. **Адаптивное вскрытие с использованием открытого текста**.

Это частный случай вскрытия с использованием выбранного открытого текста. Криптоаналитик не только может выбирать

шифруемый текст, но также может строить свой последующий выбор на базе полученных результатов шифрования.

При вскрытии с использованием выбранного открытого текста криптоаналитик мог выбрать для шифрования только один большой блок открытого текста, при адаптивном вскрытии с использованием выбранного открытого текста он может выбрать меньший блок открытого текста, затем выбрать следующий блок, используя результаты первого выбора и так далее

Существует по крайней мере еше три типа криптоаналитической вскрытия .

5. **Вскрытие с использованием выбранного шифротекста**. Криптоаналитик может выбрать различные шифротексты для дешифрирования и имеет доступ к дешифрированным открытым текстам . Например, у криптоаналитика есть доступ к "черному ящику", который выполняет автоматическое дешифрирование. Его задача состоит в получении ключа.

Дано: C_1, $P_1=D_k(C_1)$, C_2, $P_2=D_k(C_2)$, . . . C i, P i=D k(C i)

Получить: k

Такой тип вскрытия обычно применим к алгоритмам с открытым ключом. Вскрытие с использование выбранного шифротекста иногда также эффективно против симметричных алгоритмов. (Иногда вскрытие с использованием выбранного открытого текста и вскрытие с использованием выбранного шифротекста вместе называют вскрытием с использованием выбранного текста.)

6. **Вскрытие с использованием выбранного ключа**. Такой тип вскрытия означает не то, что криптоаналитик может выбирать ключ, а что у него есть некоторая информация о связи между различными ключами. Это странный, запутанный и не очень практичный тип вскрытия
7. **Бандитский криптоанализ**. Криптоаналитик угрожает, шантажирует или пытает кого-нибудь, пока не получит ключ. Взяточничество иногда называется вскрытием с покупкой ключа. Это очень мощные способы вскрытия, часто являющиеся наилучшим путем взломать алгоритм .

Различные алгоритмы предоставляют различные степени безопасности в зависимости от того, насколько трудно взломать алгоритм. Если стоимость взлома алгоритма выше, чем стоимость зашифрованных данных, вы, скорее всего, в безопасности. Если время взлома алгоритма больше, чем время, в течение которого зашифрованные данные должны сохраняться в секрете, то вы также, скорее всего, в безопасности . Если объем данных, зашифрованных одним ключом, меньше, чем объем данных, необходимый для взлома алгоритма, и тогда вы, скорее всего, в безопасности.

Ларс Кнудсен разбил вскрытия алгоритмов по следующим категориям, приведенным в порядке убывания значимости

1. **Полное вскрытие**. Криптоаналитик получил ключ, K, такой, что $D_K(C) = P$.
2. **Глобальная дедукция**. Криптоаналитик получил альтернативный алгоритм, A, эквивалентный $D_K(C)$ без знания K.
3. **Местная** (или локальная) **дедукция**. Криптоаналитик получил открытый текст для перехваченного шифротекста.

4. **Информационная дедукция**. Криптоаналитик получил некоторую информацию о ключе или открытом тексте. Такой информацией могут быть несколько бит ключа, сведения о форме открытого текста

Сложность вскрытия можно измерить различными способами:

1. **Сложность данных**. Объем данных, используемых на входе операции вскрытия .
2. **Сложность обработки**. Время, нужное для проведения вскрытия. Часто называется коэффициентом работы.
3. **Требования к памяти**. Объем памяти, необходимый для вскрытия.

Смыслом шифрования и последующего дешифрирования сообщения является восстановление первоначального открытого текста. Кроме обеспечения конфиденциальности криптография часто используется для других функций :

— **Проверка подлинности**. Получатель сообщения может проверить его источник, злоумышленник не сможет замаскироваться под кого-либо. .

— **Целостность**. Получатель сообщения может проверить, не было ли сообщение изменено в процессе доставки, злоумышленник не сможет подменить правильное сообщение ложным.
— **Неотрицание авторства**. Отправитель не сможет ложно отрицать отправку сообщения
Криптографический алгоритм, также называемый шифром, представляет собой математическую функцию, используемую для шифрования и дешифрирования.
Современная криптография решает эти проблемы с помощью ключа K. Такой ключ может быть любым значением, выбранным из большого множества. Множество возможных ключей называют пространством ключей.
Существует два основных типа алгоритмов, основанных на ключах: симметричные и с открытым ключом . Алгоритмы с открытым ключом (называемые асимметричными алгоритмами) разработаны таким образом, что ключ, используемый для шифрования, отличается от ключа дешифрирования. Ключ шифрования часто называется открытым ключом, а ключ дешифрирования - закрытым

Подстановочным шифром называется шифр, который каждый символ открытого текста в шифротексте заменяет другим символом. Получатель инвертирует подстановку шифротекста, восстанавливая открытый текст . В классической криптографии существует четыре типа подстановочных шифров :

— **Простой** подстановочный шифр, или моноалфавитный шифр, - это шифр, который каждый символ открытого текста заменяет соответствующим символом шифротекста . Простыми подстановочными шифрами являются криптограммы в газетах

— **Однозвучный** подстановочный шифр похож на простую подстановочную криптосистему за исключением того, что один символ открытого текста отображается на несколько символов шифротекста . Например, "A" может соответствовать 5, 13, 25 или 56, "B" - 7, 19, 31 или 42 и так далее.

— **Полиграмный** подстановочный шифр - это шифр, который блоки символов шифрует по группам. Например, "ABA" может соответствовать "RTQ", "ABB" может соответствовать "SLL" и так далее.

— **Полиалфавитный** подстановочный шифр состоит из нескольких простых подстановочных шифров . Например, могут быть использованы пять различных простых подстановочных фильтров ; каждый символ открытого текста заменяется с использованием одного конкретного шифра .

В **перестановочном** шифре меняется не открытый текст, а порядок символов. В простом **столбцовом** перестановочном шифре открытый текст пишется горизонтально на разграфленном листе бумаги фиксированной ширины, а шифротекст считывается по вертикали. Дешифрирование представляет собой запись шифротекста вертикально на листе разграфленной бумаги фиксированной ширины и затем считывание открытого текста горизонтально. Для него используются роторные машины. Самым известным роторным устройство является Энигма (Enigma), которая. использовалась немцами во Второй мировой войне. Сама идея пришла в голову Артуру Шербиусу (Arthur Scherbius) и Арвиду Герхарду Дамму (Arvid Gerhard Damm) в Европе. В США она была запатентована Артуром Шербиусом. Немцы значительно усовершенствовали базовый проект. Уних было три ротора

котроые можно было выбрать из пяти возможных, коммутатор, кото рый слегка тасовал открытый текст, и отражающий ротор, который заставлял каждый ротор обрабатывать открытый текст каждого письма дважды. Энигма была взломана в течение Второй мировой войны - сначала группой польских криптографов, которая объяснила раскрытый алгоритм англичанам. В ходе войны немцы модифицировали Энигму, а англичане продолжали криптоанализ новых версий.

Простое XOR представляет собой операцию "исключающее или" : '^' в языке C или Q в математической нотации. Это обычная операция над битами: $0 \oplus 0 = 0$, $0 \oplus 1 = 1$, $1 \oplus 0 = 1$,$1 \oplus 1 = 0$. Также заметим, что: $a \oplus a = 0$ $a \oplus b \oplus b = a$

Способы шифрования: одноразовый блокнот

Существует множество **компьютерных** алгоритмов. Следующие три используются чаще всего :

— DES (Data Encryption Standard, стандарт шифрования данных) - самый популярный компьютерный алгоритм шифрования, является американским и международным стандартом . Это симметричный алгоритм, один и тот же ключ используется для шифрования и дешифрирования .

— RSA (назван в честь создателей - Ривеста (Rivest), Шамира (Sharnir) и Эдлмана (Adleman)) - самый популярный алгоритм с открытым ключом. Используется и для шифрования, и для цифровой подписи.

— DSA (Digital Signature Algorithm, алгоритм цифровой подписи, используется как часть стандарта цифровой подписи, Digital Signature Standard) - другой алгоритм с открытым ключом. Используется только для цифровой подписи, не может быть использован для шифрования.

AES (Advanced Encryption Standard). Это – блочный шифр. Размеры ключа и блоков -128, 192, 256 бит, которые разбиваются на 16… сегментов по 1 байту.
InputBlock =m0, m1,…m15
InputKey = k0,k1,…k15.
Для внутреннего представления данных используется матрица 4 x 4. Далее – повторяющиеся раунды (как у DES). Преобразования внутри раунда:Round, SubBytes, ShiftRows, MixColumns, AddRoundKey. При расшифровке – в обратном порядке: $Round^{-1}$, $AddRoundKey^{-1}$, $MixColumns^{-1}$,. $ShiftRows^{-1}$, $SubBytes^{-1}$. Стр.47-55 пособия М.Л.Шилкиной.