Семестр I

Криптография с секретным ключом

1 Введение

1.1 История

Проблема защиты информации имеет давнюю историю. Везде с появлением письменности появлялась и «тайнопись» — способ преобразования информации в секретную форму, понимаемую только доверенными лицами. От греческого «$\kappa\rho\upsilon\pi\tau\sigma\sigma\ \lambda\sigma\gamma\sigma\sigma$» (тайное слово) и произошло название науки о защите информации — криптологии.

Криптология условно делится на две дисциплины: криптография — защита, и криптоанализ — атака, нападение (криптология = криптография + криптоанализ). Криптографы разрабатывают надежные (на их взгляд) системы зашиты информации, криптоаналитики пытаются найти в этих системах уязвимости. Криптографы могут гордиться тем, что атаки на действующие криптографические алгоритмы и протоколы становятся все более редкими. Криптоаналитики знают, что атаки не могут стать хуже и со временем только разовьются (attacks always get better, they never get worse).

В развитии криптологии выделяют три этапа:

1. Докомпьютерная криптология ($\leqslant 1949$). Легендарная история этого этапа — криптоанализ немецкой шифровальной машины Энигма.

2. «Закрытая» криптология (1949–76), с момента выхода в свет работы К. Шеннона «Теория связи в секретных системах». Криптология становится математической дисциплиной, потребители — дипломатические и военные организации.

3. Открытая криптология ($\geqslant 1976$, в смысле «с открытым ключом» и в смысле общедоступная, массовая), с момента выхода в свет работы У. Диффи и М. Хеллмана «Новые направления в криптографии». Криптология переносится в «цифровой мир». В цифровом мире люди хотят взаимодействовать также, как и в обычном мире. Современная криптология реашает задачи защиты информации при таком взаимодействии.

Современная криптология опирается на математику. Известно, что известный английский математик Харди, работавший в начале XX века, гордился тем, что его наука — теория чисел — никогда не будет использоваться в практических целях. Харди с удивлением узнал бы, что в современных криптографических системах используется теорема Эйлера, простые Ферма, закон квадратичной взаимности Гаусса, спаривания Вейля и другие объекты и свойства, казалось бы, чистой математики.

Современная криптографическая система — это своего рода изобретение, которое решает задачи взаимодействия между людьми в «цифровом мире». Обычные изобретения строятся на законах физики, но в цифровом мире не остается ничего другого, как использовать законы математики.

Рассмотрим некоторые понятия криптологии. Попутно будем напоминать определения нужных нам математических объектов.

1.2 Коммуникации и угрозы

Задачи защиты информации появляются при возникновении коммуникаций — обмене сообщениями между абонентами.

Абоненты — Алиса и Боб. Сообщения — слова. Обмен — канал передачи сообщений (доставка курьером, почтовое письмо, телефонная линия, Интернет-соединение).

Пусть Σ — некоторый конечный алфавит. Введем обозначения:

Σ^n — множество всех слов длины n в алфавите Σ (длина $|a|$ всякого слова $a \in \Sigma^n$ равняется n),

Σ^* — множество всех слов конечной длины в алфавите Σ (включая пустое слово $\perp$),

Σ^∞ — множество всех сверхслов (слов бесконечной длины) в алфавите Σ.

На Σ^* зададим операцию конкатенации: для $a = a_1 \dots a_n$, $b = b_1 \dots b_m$ результат операции $a \parallel b$ (или просто ab) есть $a_1 \dots a_n b_1 \dots b_m$.

Определение 1.1. *Моноидом* называется непустое множество G с бинарной операцией $*$ на нем, для которой выполняются следующие аксиомы:

1. Операция $*$ ассоциативна, т. е. для любых $a, b, c \in G$

$$a * (b * c) = (a * b) * c.$$

2. В G имеется *единичный элемент* (или *единица*) e такой, что для любого $a \in G$

$$a * e = e * a = a.$$

Упражнение 1.1. Доказать, что $\langle \Sigma^*, \| \rangle$ — моноид. □

Канал передачи сообщений является открытым, т. е. злоумышленник Виктор имеет доступ к каналу и может создавать следующие угрозы (см. 1):

– перехват сообщений (нарушение конфиденциальности);

– модификация сообщений (нарушение целостности);

– фальсификация сообщений (подделка авторства);

– прерывание передачи сообщений (нарушение доступности).

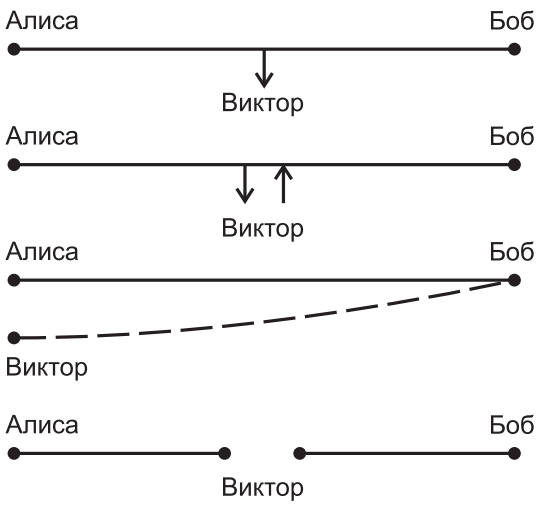

Рис. 1: Угрозы

Решения:

– организационное (ограничение физического доступа к каналу);

– инженерное (широкополосный радиоканал, квантовый канал);

– стеганографическое (скрытый или замаскированный канал);

– криптографическое — обеспечение конфиденциальности, целостности и авторства сообщений с помощью криптографических методов.

1.3 Криптосистема

Задается пятеркой $\langle \mathcal{K}, \mathcal{X}, \mathcal{Y}, E, D \rangle$, где:

$\mathcal{K}$ — множество ключей (секретных параметров);

$\mathcal{X}$ — множество открытых текстов;

$\mathcal{Y}$ — множество шифртекстов;

E — множество преобразований зашифрования $E = \{E_K \colon \mathcal{X} \to \mathcal{Y} \mid K \in \mathcal{K}\}$;

D — множество преобразований расшифрования $D = \{D_K \colon \mathcal{Y} \to \mathcal{X} \mid K \in \mathcal{K}\}$.

с ограничениями

(1) $D_K(E_K(X)) = X$ для всех $X \in \mathcal{X}$ (однозначность расшифрования);

(2) $\cup_K E_K(\mathcal{X}) = \mathcal{Y}$ (реализуемость всех шифртекстов).

Если, дополнительно, $\mathcal{X} = \mathcal{Y}$, то криптосистема называется *эндоморфной* (определение К. Шеннона). Преобразования E_K, D_K в этом случае являются биекциями $\mathcal{X}$.

Определение 1.2. Биективные преобразования $\mathcal{X}$ называются *подстановками* на $\mathcal{X}$. Множество всех подстановок принято обозначать через $S(\mathcal{X})$, а сами подстановки задавать таблицами:

$$\begin{pmatrix} a_1 & a_2 & \dots & a_{|\mathcal{X}|} \\ b_1 & b_2 & \dots & b_{|\mathcal{X}|} \end{pmatrix},$$

где a_i и b_i независимо пробегают все $\mathcal{X}$. Для $\sigma_1, \sigma_2 \in S(\mathcal{X})$ *композиция* $\sigma = \sigma_2 \circ \sigma_1$ (или просто $\sigma_2\sigma_1$) определяется по правилу:

$$\sigma(X) = \sigma_2(\sigma_1(X)), \quad X \in \mathcal{X}.$$

Множество всех подстановок на $\mathcal{X}$ с операцией композиции называется *симметрической группой*. □

Определение 1.3. Моноид $\langle G, * \rangle$ называется *группой*, если

3. Для каждого $a \in G$ существует *обратный элемент* $a^{-1} \in G$ такой, что

$$a * a^{-1} = a^{-1} * a = e.$$

Группа G — *абелева*, если

4. Операция $*$ коммутативна, т. е. для любых $a, b \in G$

$$a * b = b * a.$$

Упражнение 1.2. Доказать, что $S(\mathcal{X})$ действительно группа. Как определяется обратная подстановка? Является ли группа абелевой? □

Криптосистема C используется в следующем *протоколе* (интерактивном алгоритме).

Протокол Защищенная передача данных

Предназначен для конфиденциальной передачи слов $X \in \Sigma^*$ по открытым каналам связи

Стороны: A (Алиса), B (Боб), T (Трент, третья доверенная сторона).

Каналы: секретный канал связи (скс), открытый канал связи (окс).

Распределение ключей:

1. $T\colon K \xleftarrow{R} \mathcal{K}$.
2. $T \xrightarrow{\text{скс}} A\colon K$.
3. $T \xrightarrow{\text{скс}} B\colon K$.

Передача X:

Сценарий 1 — Блочное шифрование (используется криптосистема $\langle \mathcal{K}, \Sigma^n, \Sigma^n, E, D\rangle$)	Сценарий 2 — Поточное шифрование (используется криптосистема $\langle \Gamma, \Sigma, \Sigma, E, D\rangle$)
1. A: дополнить X до слова, длина которого кратна n, и разбить полученное слово на блоки $X_1, \ldots, X_T$. 2. A: для $t = 1, \ldots, T$: $Y_t \leftarrow E_K(X_t)$. 3. $A \xrightarrow{\text{окс}} B$: $Y_1 \parallel Y_2 \parallel \ldots \parallel Y_T$. 4. B: для $t = 1, \ldots, T$: $X_t \leftarrow D_K(Y_t)$. 5. B: собрать $X_1 \parallel \ldots \parallel X_T$, исключить дополненные Алисой символы и получить X.	1. A: записать $X = x_1 x_2 \ldots x_T$. 2. A: построить по K *бегущий ключ* $\gamma_1\gamma_2\ldots\gamma_T \in \Gamma^T$. 3. A: для $t = 1, \ldots, T$: $y_t \leftarrow E_{\gamma_t}(x_t)$. 4. $A \xrightarrow{\text{окс}} B$: $y_1 y_1 \ldots y_T$. 5. B: для $t = 1, \ldots, T$: $x_t \leftarrow D_{\gamma_t}(y_t)$. 6. B: собрать $X = x_1 x_2 \ldots x_T$.