Мотивационное письмо

Мне всегда были близки творческие занятия: пение, игра на музыкальных инструментах, креативное письмо, танцы. В детстве я посещала всевозможные секции и кружки дополнительного образования, и казалось, что передо мной открыты все дороги и пути. Так как у меня получалось всё одинаково хорошо, я распыляла себя и всё своё время на множество различных увлечений и в итоге не добилась больших успехов ни в одном из них, но узнала достаточно, чтобы быть способной поддержать разговор и даже сойти за умного человека. Всё это привело к тому, что к началу 11 класса я не имела ни малейшего представления о том, что делать дальше и куда идти, к тому же я не понимала, чего хочу от жизни, впрочем, как и многие из моего окружения. Ситуация осложнялась тем, что, не обладая какими-то углублёнными знаниями в каком-либо предмете, я не была увлечена ни одним из них, к тому же моя школа была просто не в состоянии предоставить мне, к примеру, хотя бы базовые знания по физике или информатике (попробуйте найти учителя в маленьком северном городе, у моей школы, например, не получилось). Я не видела себя ни в какой сфере, ни в какой профессии, поэтому я выбрала те экзамены, которые в принципе были лёгкими – историю и английский язык, и только потом выбрала университет. Поступив на факультет Свободных искусств и наук, я поняла, что музыка, литература, кино, философия, история и другие – это всё очень интересно, но я бы не хотела превращать эти сферы деятельности в то, что может гипотетически приносить мне доход: я хочу оставить их в своей жизни в качестве досуга. Конечно, можно сказать, что сейчас образование возможно получить и для себя, не с целью работать в сфере своего основного направления обучения. Однако я не из таких людей, и хоть я не исключаю возможность, что в дальнейшем мне будет приносить доход что-то, совершенно не связанное с компьютерными науками напрямую, я подхожу к образованию с практической и прагматической точки зрения. Именно поэтому я выбрала программу Компьютерные науки. Мне хочется верить, что именно здесь я смогу найти практические решения задач повседневной жизни, а так как наша жизнь всё больше уходит в виртуальную реальность, то владение инструментами работы с компьютером (или любой другой программируемой вещи) напрямую становится неотъемлемым условием функционирования в новой среде.

Почти за два полных года в Смольном я прослушала несколько курсов, косвенно или напрямую связанных с областью компьютерных наук. Первым таким курсом стали «Интернет-технологии», которые преподавала ещё Степанова П. П., которая во многом, наверное, привлекла меня в эту сферу (а особенно её карьерный путь в IT-сфере). Этот курс показал мне новую сторону «информатики»: это было не простой перевод

десятичных чисел в двоичное представление, а что-то совершенно для меня новое, а главное – практичное, так как мне важно понимать, как я могу применять изученную информацию в жизни и работе для решения чётко поставленных задач. Как и многих первокурсников, меня этот курс впечатлил, поэтому в следующем семестре я с нетерпением ожидала курс у Черных Г. А. «Введение в программирование и компьютерные вычисления», который оказался не столь весёлым, однако он показал мне что-то большее, чем просто вёрстку страничек и смешное оформление двигающихся картинок. В весеннем семестре первого года я также прослушала курс Князевой И. С. «Математика и информатика. Элементы математики», который мог быть более полезным, чем он стал, если бы этот семестр не был омрачён переходом на дистанционное обучение: этот период в целом был для меня достаточно тяжёлым по многим причинам. Выбранные мною курсы давались мне тяжело, и я решила попробовать экономику: она мне казалось такой же практико-направленной. Я взяла два курса по экономике, которые вымотали меня ещё больше, чем «компьютерные» курсы в начало ковидной эпохи, после чего я поняла, что у меня есть только один выбор – и это программа «Компьютерные науки и искусственный интеллект». Выбранные мною курсы в весеннем семестре второго года воспринимаются мной иначе: я сделала выбор осознанно, более-менее понимая, куда я иду. «Введение в компьютерные науки» у Жуковой А. М. и «Объектно-ориентированное программирование» у Черных Г. А. открывают для меня работу с языками программирования в ином свете, и хоть я зачастую сталкиваюсь с трудностями, я хочу их преодолеть.

В новом году я чувствую необходимость прослушать курсы Жуковой А. М. «Введение в алгоритмы», Князевой И. С. «Машинное обучение» и «Компьютерное зрение» и другие. Я стремлюсь получить как можно больше информации в стенах университета, чтобы я имела больше способов и возможностей организовать свою внеучебную деятельность, опираясь на разнообразные способы решения практических задач. Пока мне трудно определить, какая именно сфера (branch, or focus area) компьютерных наук меня интересует, собственно, из-за чего мне и хочется посетить, как можно больше курсов (как в стенах университета, так и за их пределами), для того, чтобы открыть все эти пока ещё не знакомые (или мало знакомые) мне области деятельности, которую я выбрала в качестве своей профессиональной. Меня интересуют многие направления. Так, я люблю работать с информацией и приводить её в порядок, мне нравится сортировать данные, создавать параметры, по которым можно эту информацию распределять. В то же время меня интересует то, как можно эту информацию защитить и как можно безопасно с ней работать. Также для меня представляет интерес. В принципе, я

не могу сказать, что какая-то область данного научного знания меня не интересует вовсе. Как я когда-то была в полном неведении, в какой сфере себя найти в общем, так же я сейчас в неведении, в какой области компьютерных наук я смогу найти себе применение. Найти ответ на это – моя основная задача на данным период моей жизни, и я надеюсь найти его на этой программе.

Во многом опираясь на знание своих привычек и характера, я могу отметить свой интерес к работе с данными, так как меня привлекает упорядочивание большого количества информации, сортировка и различная классификация, в том числе работа с базами данных. Впрочем, я бы не назвала это основным своим интересом, так как повторюсь, что какого-то определённого выбора я ещё не сделала. Мне также интересна область шифрования и криптографии, обзору методов и способов чего я бы и хотела посвятить свою модерационную работу.

МИНИСТЕРСТВО НАУКИ И ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образование

«Санкт-Петербургский государственный университет»

Основная образовательная программа бакалавриата

«Свободные искусства и науки»

Направление 50.03.01 «Искусства и гуманитарные науки»

Саранская Ирина Максимовна

МЕТОДЫ ШИФРОВАНИЯ

Модерационная работа

Санкт-Петербург

2021

Кто владеет информацией, тот владеет миром[*]

Сложно переоценить важность информации в современном мире. Она необходима для совершения какого-либо выбора, как в жизни отдельного человека, так и внутри какой-либо большой компании, а также на высшем государственном уровне. От достоверности, актуальности, целостности и уникальности этой информации зависит, насколько успешным будет принятое решение. В военное время от конфиденциальности информации зависят сотни тысяч, а то и миллионы, человеческих жизней. Так, дешифровка сообщений, передаваемых с помощью «Энигмы» – шифровальной машины нацистской Германии, – имела решающее значение для победы армий союзников (Richard, 1982). В повседневной жизни конфиденциальность информации также имеет большое значение для нормального функционирования банков и государственных структур. Также с помощью данных, которыми владеют различные компании, можно нанести большой урон людям и их финансам: так, банки в 300 раз больше подвержены массированным кибератакам, чем какие-либо другие организации (Zakrzewski Anna, 2019). Всевозможные сайты и поисковые системы собирают информацию, которой мы часто не придаём значения, но вот если эта информация попадёт не в те руки, это может обернуться неприятностями побольше, чем просто надоедливая таргетированная реклама. Именно поэтому так важно оберегать информацию, а главное – использовать различные методы шифровки, чтобы эти данные не оказались в руках недоброжелателя.

Эту цель люди начали преследовать задолго до создания электронных банков и Google. Криптография – одна из старейших наук в мире, история которой насчитывает около 4 тысяч лет, а способы тайного письма были известны ещё древним цивилизациями Индии, Египта и Месопотамии (Singh, 1999). Одним из самых простых и наиболее широко известных методов шифрования является шифр Цезаря, смысл которого во «вращении» каждой буквы установленное количество раз: «обратить» букву означает переместить её на определённое количество шагов (Allen, 2016). Так, А, повёрнутая 3 раза, заменяется на букву Г (Allen, 2016). Зашифрованная шифром Цезаря фраза «Beam me up, Scotty» с шагом 6 выглядит следующим образом: «Hkgs sk av, Yiuzze». Шифр является скорее хрестоматийный примером, нежели реальным шифром, способным обеспечить защиту информации, так как он легко взламывается, что объясняется небольшим количество возможных вариантов значений сдвига – всего 26 для английского языка. Конечно, к шифрованию информации в современном мире используют совершенно иные подходы.

[*] Авторство фразы приписывается и немецкому банкиру Натану Майеру Ротшильду, и британскому политическому деятелю Уинстону Черчиллю

Для того, чтобы рассмотреть методы шифрования, следовало бы наконец чётко обозначить, что же такое шифрование и какие проблемы оно решает. Шифрование – это такое преобразование информации, которое скрывало бы её от неавторизированных лиц и давало бы доступ авторизированным (Bruce, 2002). Это преобразование происходит согласно паре алгоритмов, называемых шифром. Главная задача шифрования – защита данных от посторонних лиц, т.е. сохранение конфиденциальности информации, а также защита данных от несанкционированного изменения. Шифрование также используется для сохранения важной информации в ненадёжных источниках и её передачи по открытым, незащищённым каналам связи. Шифрование информации происходит с использованием особого ключа, который и отвечает за «сохранение» в себе алгоритма шифровки и/или дешифровки (Maiwald, 2001). Процесс передачи зашифрованной информации представлен двумя процессами: зашифровыванию на одном конце передачи и расшифровыванию на другом. Авторизованным пользователем, который имеет доступ к информации, является обладатель аутентичного (т.е. действительного и подлинного) ключа. В зависимости от того, сколько ключей используется, применяются разные методы шифрования: симметричное и ассиметричное шифрование. До 1976 года использовались только одинаковые ключ и для зашифровывания, и для расшифровывания, но затем американцами У. Диффи и М. Хеллманом был предложен новый принцип построения криптосистем, не требующий передачи ключа принимающей стороне (Гатчин & Коробейников, 2002). Симметричные и асимметричные способы шифрования данных обладают как преимуществами, так и недостатками, что определяет область применения того или иного метода. Так, благодаря лучшей производительности и более высокой скорости симметричное шифрование обычно применяется для массового шифрования больших объёмов данных и используется, например, в банковском секторе в платёжных приложениях, где личная идентификационная информация должна быть защищена для предотвращения кражи личных данных (Smirnoff & Turner, 2019). Также симметричное шифрование применяется для шифрования неактивных данных, т.е. таких данных, которые не перемещаются с устройства на устройство или из сети в сеть, а хранятся на жёстком диске или любом другом носителе, устройстве или сети (Arampatzis, 2019). Асимметричное же шифрование решает проблему передачи ключа по незащищённому каналу.

Симметричные алгоритмы шифрования основаны на том, что отправитель и получатель используют один и тот же ключ (Гатчин & Коробейников, 2004), поэтому сохранение секретности ключа – важная задача для установления и поддержания канала связи. Симметричное шифрование также называют криптографией с секретным ключом,

так как этот ключ должен держаться в тайне для успешного обмена информацией. Схема реализации симметричного шифрования выглядит примерно следующим образом:

Два абонента – Алиса и Боб – хотят обменяться информацией (Menezes, van Oorschot, & Vanstone, 1997)

Генерация ключа	Зашифровывание и передача данных	Расшифровывание сообщения
Алиса выбирает ключа шифрования k и пару алгоритмов C и D и передаёт эту информацию Бобу	Алиса шифрует сообщение m с использованием ключа k и алгоритма C, получая на выходе шифротекст c, $C(m,k)=c$ который и передаёт Бобу	Боб с помощью того же ключа k и алгоритма D расшифровывает шифротекст c, получая на выходе первоначальное сообщение m $D(c,k)=m$

Таблица 1. Схема реализации симметричного шифрования

Таким образом, можно выделить достоинства и недостатки симметричного шифрования. К достоинствам можно отнести относительную простоту реализации обмена информации, а также более высокую скорость, с которой осуществляется шифровка/дешифровка; самым большим недостатком и уязвимым местом является передача ключа, так как при перехвате ключа третьей стороны злоумышленник получает доступ не только к чтению информации, но и к её изменению.

Решить проблему передачи ключа помогает ассиметричная система шифрования, или система с открытым ключом, в которой используется два ключа – открытый и закрытый, связанные друг с другом определённым образом. Открытый ключ передаётся по незащищённому каналу связи, и третье лицо может получить к нему доступ. Однако с помощью этого ключа можно только зашифровать сообщение или проверить электронную подпись (то есть проверить авторство какой-либо информации, но не подтвердить его или сгенерировать). Для генерации такой подписи или расшифровывания сообщения используется уже закрытый ключ (Bruce, 2002). Схема реализации асимметричного шифрования для передачи сообщения ***в одну сторону*** выглядит примерно следующим образом:

Два абонента – Алиса и Боб – хотят обменяться информацией (Menezes, van Oorschot, & Vanstone, 1997)

Генерация ключевой пары	Зашифровывание и передача данных	Расшифровывание сообщения
Боб выбирает алгоритм (E и D) и пару ключей	Алиса шифрует сообщение m с использованием открытого ключа e,	Боб с помощью закрытого ключа d

(e, d) и посылает Алисе открытый ключ e по открытому каналу	получая на выходе шифротекст c, $E(m, e) = c$ и передаёт его Бобу	расшифровывает шифротекст c $D(c, d) = m$

Таблица 2. Схема реализации асимметричного шифрования для передачи сообщений в одну сторону

Если необходимо наладить канал связи для работы в обе стороны, то требуется провести первые две операции (Генерацию ключевой пары и Зашифровывание и передачу данных) для обеих сторон. Каждый участник коммуникации будет знать три ключа: два своих – закрытый и открытый, а также открытый ключ собеседника, при этом закрытый ключ остаётся в секретности. Несмотря на кажущуюся безопасность ассиметричного шифрования, в неё может вторгнуться перехватчик (в условных обозначениях взаимодействующих агентов в криптографии такой пассивный перехватчик имеет имя Ева, от англ. eavesdropper – подслушивающий), который может захватить всю систему без её непосредственного взламывания (Menezes, van Oorschot, & Vanstone, 1997). На рисунке представлена модель перехвата открытого ключа, а в таблице описана реализация перехвата сообщения третьи лицом.

Два абонента – Алиса и Боб – хотят обменяться информацией, но Ева вмешивается в их коммуникацию (Menezes, van Oorschot, & Vanstone, 1997)

Генерация ключевой пары	Перехват ключа и зашифровывание данных	Перехват шифротекста и его «вскрытие»	Расшифровывание сообщения
Боб выбирает алгоритм (E и D) и пару ключей (e, d) и посылает Алисе открытый ключ e по открытому каналу	Ева перехватывает открытый ключ e и создаёт пару ключей e' и d', «маскируясь» под Боба. Алиса зашифровывает сообщение m $E_{e'}(m) = c'$ и отправляет Бобу шифротекст c'	Ева перехватывает шифротекст c' и расшифровывает его с помощью секретного ключа d' $D_{d'}(c') = m,$ заново шифрует открытым ключом Боба e $E_e(m) = c$ и отправляет шифротекст c Бобу	Боб с помощью закрытого ключа d расшифровывает шифротекст c $D_d(c) = m,$ не догадываясь при этом, что сообщение было перехвачено

Таблица 3. Схема реализации перехвата сообщения третьим лицом

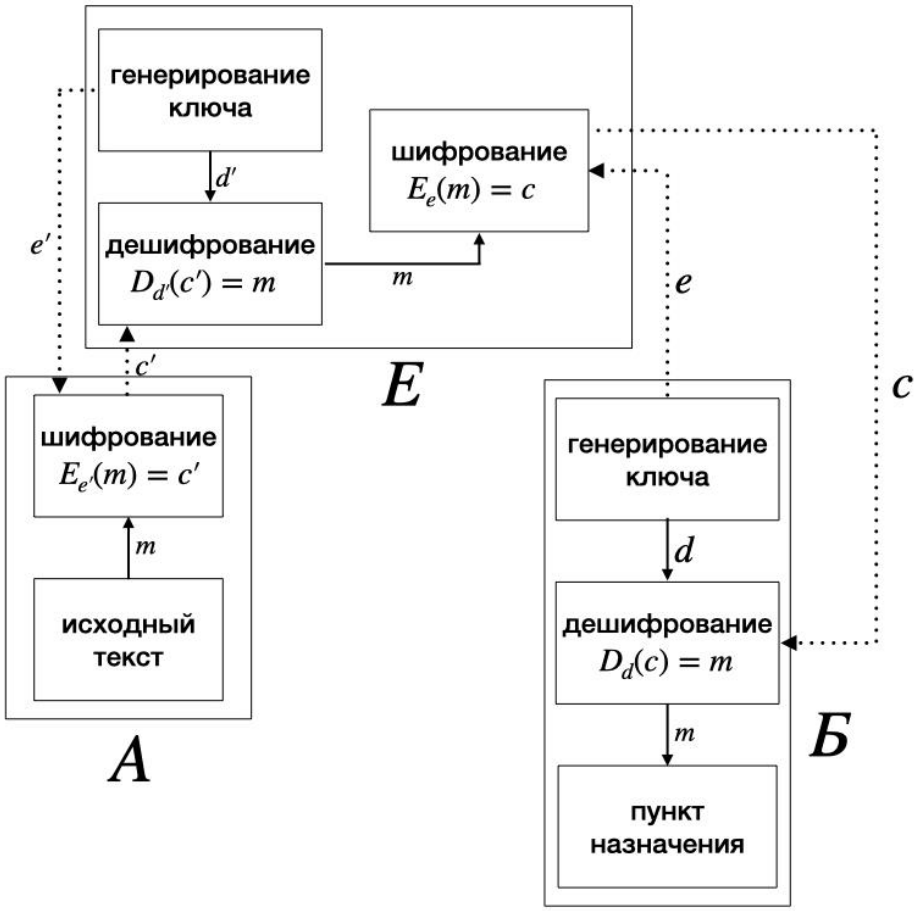

Схема 1. Схема перехвата сообщения третьим лицом

Таким образом, никто из участников коммуникации не знает о «третьем лишнем», который может не просто перехватить сообщение и узнать о его содержимом, но и подменить его на ложное сообщение *m'*. Для решения этой проблемы были внедрены сертификаты открытого ключа. Они содержат информацию о владельце открытого ключа и область его применения и подтверждают принадлежность данного ключа владельцу. Помимо такого перехвата, асимметричное шифрование может подвергаться и другим формам атаки. Несмотря на это, асимметричные шифры имеет ряд преимущества перед симметричными (Menezes, van Oorschot, & Vanstone, 1997):

1. Не нужно предварительно передавать секретный ключ и обеспечивать надёжность канала для передачи этого ключа
2. Многие схемы с открытым ключом обеспечивают относительно эффективные механизмы электронной подписи
3. В крупных сетях число ключей значительно меньше

Однако асимметричное шифрование имеет и свои недостатки, такие как медленная скорость зашифровывания/расшифровывания по сравнению с симметричным шифрованием, более длинные ключи (для систем с аналогичной криптостойкостью длина асимметричных ключей в 6-8 раз больше), а также бóльшие вычислительные затраты.

Симметричный и ассиметричный методы шифрования зачастую применяются совместно (или скорее последовательно), устраняя таким образом недостатки друг друга и обеспечивая максимально возможную конфиденциальность информации. Приложения для обмена сообщениями, такие как WhatsApp или Telegram, используют сквозное шифрование (end-to-end encryption) для защиты конфиденциальности сообщений и аутентификации пользователей. Такое шифрование реализовано с помощью обоих типов шифрования, рассмотренных выше. Так, с помощью ассиметричного шифрования инициализируется коммуникация между пользователями, а симметричное шифрование используется на протяжении самой коммуникации (Arampatzis, 2019). Похожему принципу работы подчиняется и HTTPS-соединение. HTTPS – это расширение протокола передачи данных HTTP, которое поддерживает шифрование в целях повышения безопасности. Такой тип соединения так же устанавливается изначально с помощью асимметричного шифрования, а поддерживается уже с помощью симметричного шифрования, которое генерирует ключ сеанса – одноразовый симметричный ключ, используемый в одном сеансе связи. Таким образом, использование различных методов шифрования на разных этапах соединения решает, во-первых, проблему медленной скорости и больших трат ресурсов центрального процесса асимметричного шифрования, а во-вторых, проблему распределения ключей, возникающих при симметричном шифровании (Arampatzis, 2019).

Симметричный и асимметричный методы шифрования, являясь основными способами шифрования, не являются единственными исходя из того, что многообразие информации, которое мы имеем на сегодняшний день, и глубокое проникновение информационных технологий в устройство наших жизни требует разнообразные способы их шифровки. Помимо вышеописанных методов, существует множество способов защиты данных, выбор которых зависит от расположения данных, того, что именно с ними происходит (они хранятся на устройстве, передаются, располагаются на сервере), необходимого уровня защиты и много другого. Симметричные и асимметричные методы шифрования, описанные в работе, применяются повсеместно, и современный человек уже редко может их избежать в своей повседневной жизни, так как они обеспечивают защиту данных, передаваемых человеком ежедневно. По мере совершенствования методов шифрования, методы взлома различных шифров также развиваются, поэтому главная задача, стоящая перед криптографией сейчас, – это постоянный поиск, анализ, а главное разработка таких методов шифрования, которые бы смогли максимально обеспечить безопасность важных данных и информации.

Список источников

1. Rejewski Marian, Woytak Richard (1984), A Conversation with Marian Rejewski. Westwood, Praeger
2. Zakrzewski Anna, Tang Tjun, Appell Galina, Hardie Andrew, Hildebrandt Nicole, Kahlich Michael, Mende Martin, Muxí Federico, Xavier André (2019), Global Wealth 2019: Reigniting Radical Growth. Boston, BCG
3. Singh Simon (1999), The Evolution of Secret Writing // The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography. New York, Doubleday
4. B. Downey Allen (2016), Think Python, 2nd Edition. Boston, O'Reilly Media
5. Schneier Bruce (1996), Applied Cryptography. Protocols, Algorithms and Source Code in C. New York, John Wiley & Sons
6. Maiwald Eric (2001), Network Security: A Beginner's Guide. Berkeley, Osborne/McGraw-Hill
7. Коробейников Анатолий, Гатчин Юрий (2004), Математические основы криптологии. СПб, СПб ГУ ИТМО
8. Коробейников Анатолий, Гатчин Юрий (2002), Основы криптологических алгоритмов СПб, ГИТМО (ТУ)
9. Menezes Alfred J., van Oorschot Paul C., Vanstone Scott A. (1997), Handbook of Applied Cryptography. Boca Raton, CRC Press
10. Smirnoff Peter, Turner Dawn M. (2019), Symmetric Key Encryption. Aarhus, Cryptomathic
11. Arampatzis Anastasios, Use Cases for Symmetric and Asymmetric Encryption (2019)