

Информатика



Душкин Роман Викторович
 Директор по науке и технологиям
 Агентства Искусственного
 Интеллекта



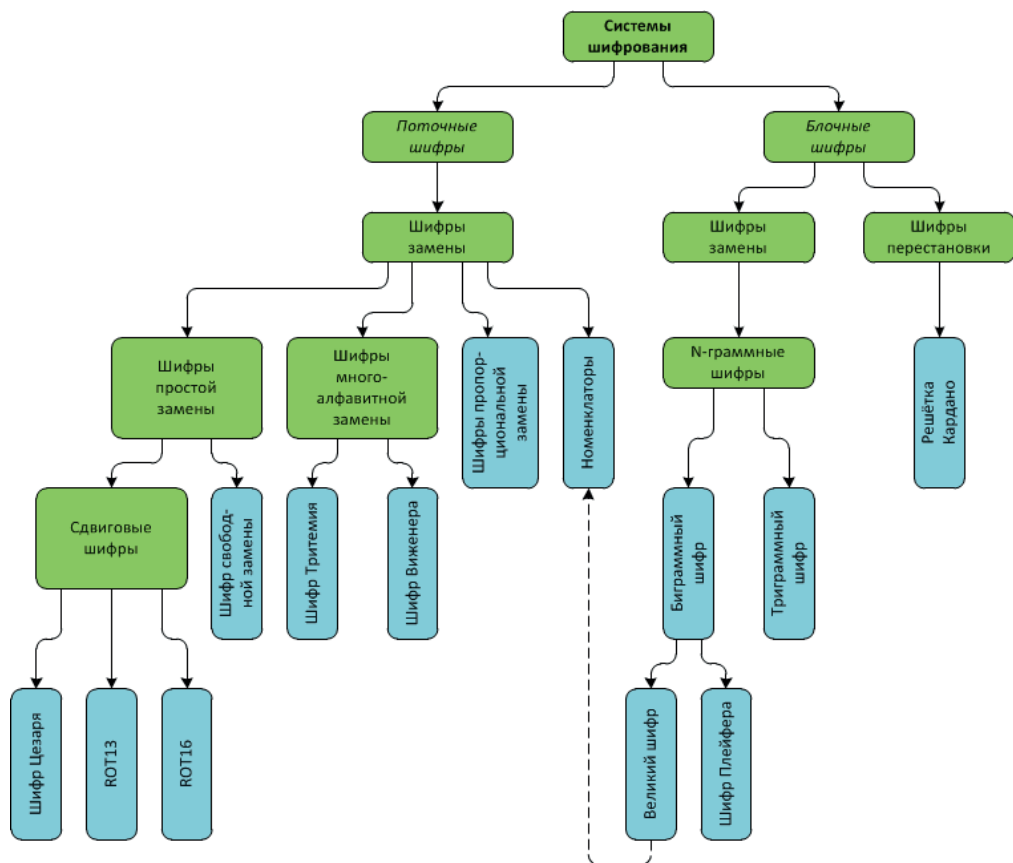
Яхонтов Светозар Игоревич
 Директор по развитию
 компаний StarForce и Safe'n'Sec,
 эксперт по информационной безопасности.

Номенклаторы

Мы продолжаем наш цикл статей по криптографии, и это статья, в которой мы изучим новое понятие, имевшее важное значение в старинных методах шифрования – это номенклаторы. Сегодня они практически не используются, однако в прошлом номенклаторы имели существенный вес в криптографических системах, так что их изучение полезно, хотя бы с той точки зрения, что если вам попадётся древний документ, в котором они используются, вы будете знать, с чем имеете дело.

Ну что ж, мы уже изучили большое количество методов шифрования (и атаки на них) – поточный и блочные типы шифров, шифры замены и шифры перестановки. Скоро мы перейдём к совершенно иной области работы с информацией, ну а пока закрепим в памяти всё, изученное ранее, и узнаем специальный метод шифрования, который в области профессиональной защиты информации сегодня практически нигде не используется, но вы можете успешно применять его для сокрытия своих секретов при обмене ими с доверенными лицами. Здесь речь идёт о так называемых номенклаторах.

Номенклатор – это простой словарь, в котором каждому кодовому слову сопоставляется какой-то специальный смысл. Поэтому, номенклаторы можно использовать в качестве ключей для кодирования информации. При этом под термином «кодирование» информации мы понимаем применение специальных обозначений на любом уровне, в том числе и на уровне единиц текста, обладающих смыслом. То есть кодировать мы можем, и слова, и предложения, и даже целые тексты. Также кодировать можно и отдельные буквы, так что любой шифр является кодом, но не каждый код может быть шифром.



Мы актуализируем диаграмму, которую составляем с самого начала нашего цикла. Теперь в ней появился новый тип стрелки – пунктирная. Пунктирная стрелка обозначает, что

какой-то шифр использует другой. А при помощи цветовой разметки показываются классы шифров (зелёные) и конкретные шифры (голубые).

Первые упоминания номенклаторов

Есть мнение, что одними из древнейших сохранившихся документов, составленных с применением номенклаторов, являются труды древних шумерских астрологов (III тысячелетие до нашей эры). Документ, обращённый к правителю Аккада (город-государство в Древней Месопотамии), предвещал полное лунное затмение и предупреждал

правителя о возможной смене власти, как то было в предыдущие аналогичные затмения, прошедшие за 65 лет.

Для того чтобы заметить, что лунные затмения определённого типа предвещают смерть правителя, шумерам уже тогда нужно было иметь записи наблюдений за небом. Используемые в астрологии и те-

перь в современной астрономии символы, обозначающие планеты Солнечной системы, также дошли до нас из цивилизации древних шумеров.

Примечательно, что в арабском языке, который имеет заимствования из аккадского и других шумер-

ских диалектов (большая часть арабских государств располагается на территории бывшей Месопотамии), значения и даже произношения слов, обозначаемых одним астрологическим символом, либо схожи, либо вовсе совпадают.

Таблица 1. Символы планет в астрологии и современной астрономии, заимствованные из арабского языка

Символ	Небесное тело	Металл	Значение символа в арабском языке	Значение слова в арабском языке
♿	Меркурий	Ртуть	Стилизованное сокращённое перевёрнутое набок написание арабского слова «Меркурий» (عطارد – «Утарид»)	Жидкое серебро
♀	Венера	Медь	Название Венеры по-арабски, сокращённое до первой буквы и стилизованное (الزهرة – «Зухра»)	Блеск, красота
♂	Марс	Железо	Стилизованное сокращённое перевёрнутое написание арабского слова «Марс» (المريخ – «Аль Мерикх»)	Козёл (в значении «пастух овец» или «пастух небесных тел»)
♃	Юпитер	Олово	Стилизованное сокращённое написание арабского слова «олово» (المشتري – «Аль Мукшери»)	Юпитер, олово, покупатель
♄	Сатурн	Свинец	Название Сатурна по-арабски, сокращённое до первой буквы и стилизованное (زحل – «Зхльнун»)	Созидатель, сеятель (стекловидная свинцовая глазурь использовалась в качестве покрытия на водонесущих керамических поверхностях акведуков, используемых для орошения полей)

Так в арабском языке слова «покупатель» и «олово» (аль мукшери), как полагают историки, имеют родственные корни вследствие особого значения олова в Бронзовом веке – времени существования цивилизации шумеров. Олово – один из компонентов бронзы (бронза на 85 % состоит из меди и на 15 % из олова). Олово в Бронзовом веке было стратегическим металлом. Имея олово, можно было производить оружие из бронзы и вооружать армию, что обеспечивало государству шумеров влияние в регионе и существование их цивилизации. При этом на территории Месопотамии не было месторождений олова (в то время его добывали исключительно в чистом виде – в виде самородков). Ближайшие месторождения самородного олова

были в Африке. И единственным источником пополнения его запасов была торговля. Слово «покупатель» имело смысл «тот, кто меняет на олово».

Так и многие в нашей цивилизации технологии, доступные повседневно, создавались часто именно для военных нужд. В этом виде деятельности наиболее явно проявляются результаты сочетания нужды в преодолении ограничений и наличия политической воли. А распространение достижений происходит вследствие развития торговли и, соответственно, конкуренции, в том числе в весьма агрессивных формах. Потому историю шифров интересно рассматривать в контексте военной истории и истории развития торговых отношений.

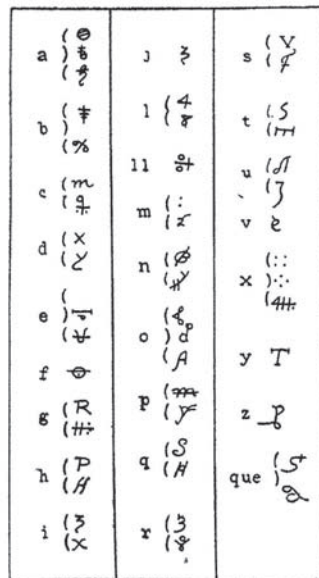
Номенклаторы в шифровании XIV–XV веков

Номенклаторы как один из видов формальной криптографии, используемой для сокрытия смысла послания, получили распространение к концу XIV века. К этому времени развитие науки и торговли вызвало спрос на относительно стойкие к ручному криптоанализу шифры. А торговые войны на новых территориях между итальянскими городами-государствами стали драйвером распространения методов шифрования, разработанных в предыдущие столетия в арабских странах в период завоевания ими Пиренейского полуострова и крестовых походов. Именно тогда были написаны первые труды по (как говорим теперь) анализу криптостойкости и частотному криптоанализу. Отсутствие технологий печатного дела и практики запрета

«алхимии и колдовства» католической церковью позволяли одновременно широко использовать нестойкие к частотному криптоанализу шифры и в порядке частных научных исследований развивать методологии криптоанализа.

Также шифрограммы с применением номенклаторов использовались для тайных посланий испанскими конкистадорами в период завоевания Америки.





Receivendo o livro, o Sr. João Ribeiro, em 25 de maio de 1930, escreveu:

державой, занимающей огромную территорию от Днепра на западе до Тихого океана на востоке. Государство – это в первую очередь канцелярия и учёт. И для организации эффективного управления огромной территорией была необходима быстрая, надёжная и конфиденциальная связь.



Шифровка послания составлена персонально императором Петром Алексеевичем и адресовалось, видимо, князю Долгорукову, подавлявшему мятеж на Дону. Оно предписывало бунтовщиков «истребить» и себя от подобных «оглядов ... учинить»

В 1740-е годы в России начинают свою работу «чёрные кабинеты». В этих учреждениях службы перлюстрации проводилась сложная процедура вскрытия всей дипло-

матической корреспонденции иностранных представительств, дешифровка, и, подчас, подмена содержания послания с последующим шифрованием.

Конец широкого применения номенклаторов для сокрытия смыслового содержания посланий

В 1863 г. Фридрих Касиски опубликовал метод, впоследствии названный его именем, позволяющий быстро и эффективно вскрывать практически любые шифры того времени. Метод состоял из двух частей – определения периода шифра и

дешифровки текста с использованием частотного криптоанализа.

Распространение этого научного труда в скором времени положило конец использованию шифров на основе замены в целях сокрытия информации.

Современное применение номенклаторов

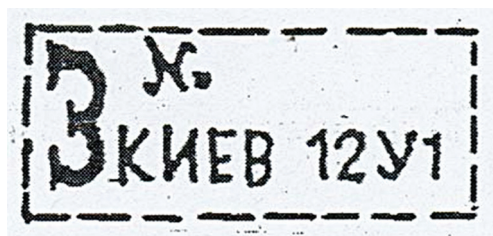
В современном мире номенклаторы используются именно для сокращения времени передачи или восприятия информации. Примером повседневно применяемых номенклаторов являются почтовые индексы. Почтовые индексы – буквенно-числовые обозначения, добавляемые к почтовому адресу с целью облегчения сортировки почтовых отправлений. Причиной появления почтовых индексов стал рост численности населения в крупных городах, связанный с урбанизацией экономики государств и соответственно с воз-

росшей сложностью сортировки почтовых отправок между множеством почтовых отделений одного города.

Именно беспрецедентно высокие темпы индустриализации первой пятилетки на территории Украинской ССР привели к росту городского населения республики на 2,6 млн человек, что стало одной из причин создания на территории УССР системы почтовых индексов, которую в том или ином виде в последующие десятилетия XX века переняло большинство стран мира.

Таблица 2. Формат почтовых индексов СССР 1930-х годов

12	У	1
обозначение города	«У» – Украина	Номер почтового отделения в городе
01-10 – Харьков 11-20 – Киев		



Штамп заказного письма с указанием почтового индекса 12У1
(Киев, СССР, 1930-е годы)

В 1939 году когда (уже шла Вторая мировая война, к СССР были присоединены территории Западной Украины и Западной Белоруссии, началась Советско-Финской война 1939 – 1940 годов),

систему почтовых индексов в СССР упразднили. Некоторое время на новых присоединённых территориях СССР действовали системы почтовых индексов Польши и Финляндии.

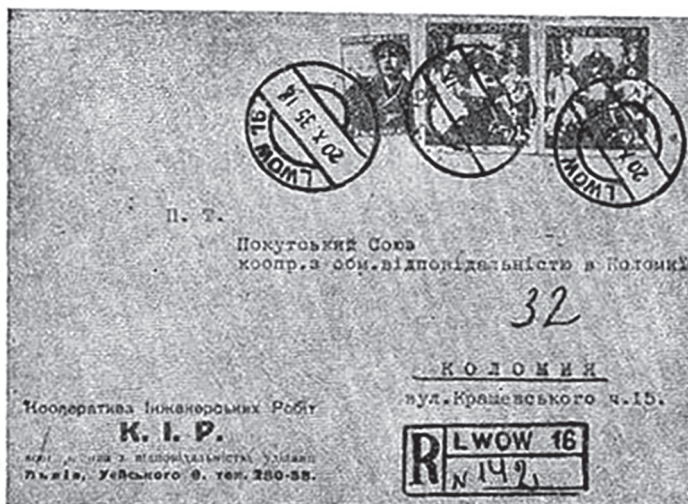


Рис. 1. Заказное письмо, сданное 20. X. 39 в п. о. Львов-16. Смешанная франкировка по польскому тарифу. На обороте штемпель прибытия: «kotomyia *m* 21. X.39.21».



Рис. 2. Заказное письмо, сданное 21. X. 39 в п. о. Дрогобыч-1. Смешанная франкировка по польскому тарифу. На обороте штемпель прибытия: «L wów—1 *2K 22.X.39.10».

Современная система почтовых индексов, действующая на территории Российской Федерации, была введена в СССР в 1971 году. В настоящее время в России принята 6-значная система XXXYYY, где XXX – код города, а YYY – номер почтового отделения, однако многие крупные города, такие как, например, Москва или Санкт-Петербург, имеют несколько кодов города. Примечательно, что отдельные индексы могут принадлежать отдельным организациям. Так, индекс 123100 принадлежал Дому правительства Российской Федерации.

Также примером повсеместно используемого номенклатора является

товарный штрихкод. Целью данного шифра не является сокрытие информации от покупателя товара. Обыватель из этого шифра сможет узнать только страну производства. Для получения информации о производителе потребуется иметь справочник, состоящий из тысяч записей. Цель применения штрихкодов заключается в автоматизации ввода данных о движении единиц товара. Это позволяет планировать нормы товарных запасов, ритмичность поставок, что крайне важно для обеспечения доступности товаров с небольшими сроками годности (не содержащих консерванты, не подвергнутых термической обработке).



Согласно той или иной системе, каждому виду изделия присваивается свой номер, состоящий чаще всего из 13 цифр (EAN-13).

Структура товарного 13-ти значного штрихкода системы EAN-13

Современное применение номенклаторов в бытовом общении и деловой переписке

Развитие Интернета и появление интернет-форумов, социальных сетей и мессенджеров породило целый язык сокращений, которые также являются номенклаторами.

- IMHO – in my honest opinion, что в переводе означает «по моему скромному мнению».

- LOL – laughing out loud, что в переводе означает «громко смеюсь».

Даже смайлики, передающие эмоциональную часто, смысловую нагрузку акта коммуникации, являются номенклаторами.

Многое из интернет-сленга перекочевало и в корпоративную электронную переписку:

- FYI – for your information (для информации).

- ASAP – as soon as possible (как можно скорее).

Метод шифрования

Для кодирования номенклаторам важно определить используемые

справочники или «шифровальную книгу», из которой будут взяты сло-

ва и символы для замены. И, конечно же, договориться об использовании таких источников с партнёром по переписке.

Все мы наблюдали в голливудских фильмах сцены переговоров полиции: «всем патрулям: 10-99...». Примечательно, что полицейские из разных штатов или даже городов одного штата могут использовать разные справочники кодов. Так, полицейский департамент Окленда, будучи самым передовым по большинству показателей подготовки офицеров полицейским департаментом в США, первым перешёл на новые «11-е коды». Спустя год полицейские департаменты других графств Калифорнии перешли на «10-е коды».

Для усложнения способов декодирования посланий можно использовать редкие справочники. Так, в период Второй мировой войны Военно-Морские Силы США использовали для кодирования посланий редкий язык индейского племени навахо. До 1950-х годов не было издано ни одного научного труда по этому редкому языку, студенты из Германии, проходившие обучение в США, с 1922 года, не имели зафиксированных контактов с носителями этого языка (или изучавшими язык), которых на 1942 год было всего 26 человек. И даже догадавшись о том, что для кодирования применяется именно этот редкий язык, противник не мог обратиться к готовому справочнику (словарю) для проведения расшифровки.

Методы атаки

Как, вероятно, догадался вдумчивый читатель, для декодирования зашифрованных номенклаторами посланий в случае шифров простой замены, применим метод частотного анализа, с которым вы уже ознакомились в предыдущих статьях. Трудности могут возникать в случае включения в зашифрованное послание слов-пустышек, намеренных ошибок, недостаточности объёма

текстов для построения частотной диаграммы и применения нескольких взаимопересекающихся справочников с правилами чередования.

Способы получения шифрованной книги противника, выведывания информации о применяемых справочниках посредством шпионажа интересны с исторической точки зрения, но в этом цикле статей не рассматриваются.

Заключение

Применение номенклаторов в современной повседневной жизни стало обоснованной необходимостью. Современную логистику (военную и торговую, управление движением товаров и транспортировкой, информационную логистику и т. д.) невозможно представить без кодиро-

вания информации номенклаторами. XXI век является веком логистики и глобализации, сквозной информатизации и кросс-компетенций во всех сферах деятельности.

Необходимо расширять кругозор за рамки своей профессиональной области, находить и создавать связи

со смежными и новыми видами деятельности. Необходимо уметь создавать и изучать новые языки, кото-

рые будут «сшивать» информационные потоки «лоскутного одеяла» новой цивилизации.

Упражнения

В качестве домашнего задания и самостоятельных упражнений рекомендуем:

- Прочитайте книгу Татьяны Соболевой «История шифровального дела в России».

1. Определите какое географическое название закодировано астрономическим номенклатором в выражении с почтовыми номенклаторами: **2705-001 < 2П < 618871**? Для этого можно воспользоваться такими подсказками:

- о Укажите, из каких открытых публикуемых справочников были взяты эти номенклаторы.

- о Определите, какие топографические объекты заданы почтовыми номенклаторами.

- о Установите, границы какой территории заданы этими топографическими объектами.

- о Проверьте полученный результат, расшифровав название астрономического объекта, заданного номенклатором **2П**

2. Создайте собственный справочник номенклаторов. Это может быть список упражнений из плана спортивных тренировок. Или указатель регулярных маршрутов, по которым вы перемещаетесь. Или перечень обыкновенно покупаемых продуктов и предметов быта в супермаркете. Или любой другой справочник предметов, действий, событий которые вы наблюдаете регулярно.

3. Реализуйте на своём любимом языке программирования утилиту, которая для заданного текста и словаря номенклаторов возвращает шифrogramму этого текста.

Калейдоскоп Калейдоскоп Калейдоскоп

На Физтехе прошел первый международный хакатон по Android и Web-разработке

В МФТИ прошел Local Hack Day – первый международный хакатон по Android и Web-разработке на Физтехе. Организатором стал проект бизнес-акселератора МФТИ Phystech.Genesis, партнером – компания HERE Technologies.

Local Hack Day – это 12-часовой хакатон, объединяющий техников-энтузиастов в единое сообщество: начинающие программисты, дизайнеры и менеджеры вместе работают над решением какой-либо задачи. Соревнование проходит с фокусом на образовательную часть.



Источник: <https://mipt.ru/news>