**Лекция за 22.02.2012, часть 2**

***Теоретические основы вопросов, связанных с передачей данных на расстояние. Исторический экскурс.***

Код Enigma был вскрыт в 1942 англичанами. Они поделились им (кодом) с американцами в 1943 году, и отказались делиться с Советским Союзом. Во второй половине 1944 года после выставки в Нормандии Черчилль предложил Сталину поделиться секретом Enigma. Сталин отказался, сказав: «Хорошо ещё как в христовы дни нам уже не надо». Означает ли это то, что на тот момент Советский Союз мог сам расшифровать код Enigma, либо это был такой дипломатический отказ, который демонстрировал обиду Сталина - до сих пор неизвестно.

***Юрий Кнорозов*** *- первый человек, который прочитал письменность майя. Он умер в начале 2000х годов. Во время войны он посещал лингвистический кружок при Московском гос-м университете и соответственно поступил потом туда на отделение лингвистики. Буквально незадолго до его смерти (умер он в 2002 году), стало известно, что во время войны он входил в группу лингвистов-математиков, которые занимались дешифровкой немецких шифров (кроме энигмы были и другие шифры). Отчасти эта секретность связана с тем, что по советским законам эти все секретные документы не деклассифицировались в течение 50ти лет. То есть как раз 50 лет с момента окончания войны(1995 год). Сколько же всего чудного ждёт нас в архивах.*

Код, который использовался в Enigma, относится к разновидности ***полициклических шифров***. Машина Enigma представляла собой следующее: в ней было 4 коммутационных диска, которые могли ставиться в произвольное положение. Соответственно, было 24 в 4й степени разных вариантов на неповторяющиеся шифры последовательностей. Осуществлялась электромеханическая коммутация, то есть внешне это выглядело так: было две пи-машинки, подключённых электрическими проводами к некой коробочке, в которой эти диски и находились. На одной пи-машинке набирали исходный текст, а вторая пи-машинка на бумаге (или каким-нибудь иным способом) воспроизводила текст уже зашифрованный. Одно из особенностей, которое влияло в лучшую сторону на криптостойкость, было то, что 4й из этих дисков был сменный, и, теоретически, на каждый день был свой диск. Мало того, что количество кодовых комбинаций было очень велико, но и один из ключевых дисков каждый раз заменялся, что очень хорошо развивало все статистические особенности шифротекста.

***На чём была построена расшифровка Энигмы?*** Во 1-х в одной из операций английских ВВС была потоплена немецкая подводная лодка, с которой удалось снять практически не повреждённую Энигму. Причём в инструкциях по действиям в случае потопления корабля первым пунктом всегда стояло: необходимо уничтожить шифромашину. Она была более менее разборная, то есть её надо было разделить на несколько кусков и по возможность выбросить за борт в разные стороны. Здесь же немцы с лодки сбежали, не выполнив самого первого пункта по поведению в аварийной ситуации. После этой операции стало примерно ясно, как работает Enigma, но всё равно не до конца. Не получилось разобрать всю схему коммутаций, т.к. там использовалась часть материала, довольно быстро разрушаемого морской водой.

На самом деле получив машинку, они получили код на один день. После этого начали работу британские математики. *Здесь был один тонкий момент: многие работы 20-го века по криптоанализу делались на основе математических взысканий венской математической школы. В этой венской матшколе было много поляков. И так получилось, что во время войны по разные стороны фронта с этим вопросом работало аномально много поляков (т.е. много поляков работало в Англии, часть поляков работала в СССР, часть в Америке, и возможно даже в Германии). Скорее всего, в венской школе также находились и чистокровные немцы. Венская математическая школа сыграла огромную роль в криптоанализе. После войны по нашу сторону железного занавеса венская матшкола почему-то называлась польской.*

Соответственно, были использованы две вещи: немецкий язык, как и любой германский язык, очень регулярный. В любом немецком тексте есть большое количество повторяющихся фрагментов, особенно в началах предложений. (Если бы при помощи Энигмы шифровали бы русский текст, получилось бы всё не так гладко, т.к. русский язык гораздо более безалаберен: нет устойчивого порядка слов в предложении, очень много флективных форм, которые заметно разбивают статистические особенности текста и т.д.)

Вторая особенность была в том, что англичане перехватывали радиосообщения с подводными лодками. Кому-то пришла в голову очень интересная мысль, что немцы должны были в этих сообщениях передавать прогнозы погоды. Т.е. Фактически удалось в определённый момент времени построить расшифровку с использованием известного не зашифрованного текста (можно было хотя бы предположить, как этот не зашифрованный текст выглядит).

Кроме того, был использован ещё один момент: немецкие лодки обычно задерживались в море дольше положенного им срока (пока у них там ещё припасы не заканчивались). Поэтому загруженные 4е шифродиски у них заканчивались, и они начинали пользоваться повторно уже имеющимися. И это позволило восстановить некоторую статистику. В итоге дело закончилось тем, что над расшифровкой бились примерно год. В течение года удалось построить алгоритм дешифровки (основанный в основном на переборе). Также удалось построить механическую дешифровальную машину, которая получала в распоряжение шифротекст, в большом количестве крутила колёсиками и пыталась подобрать, шифруя короткие 3х и 4х буквенные слова, так, чтобы были похожие на них сочетания в известном шифротексте. В венской школе также находились и чистокровные немцы. Венская математическая школа сыграла огромную роль в криптоанализе. После войны по нашу сторону железного занавеса венская матшкола почему-то называлась польской.

Ко второй половине войны англичане научились расшифровывать практически 80% сообщений. В конце войны немцы добавили 5й шифродиск, т.к. количество потерь подводных лодок начало говорить о том, что англичане уже что-то знают. 5й шифродиск на самом деле уже мало кому помог, хотя Энигму с 5ю дисками до конца войны так и не расшифровали. Англичане после войны наладили постановку Энигмы на поток и использовали в бывших колониях до конца 60х-70х годов. Но в основном уже не для дипломатической связи, а возможно для бюрократической и коммерческой переписки.

*Английская модификация использовала уже 6 дисков, из которых были три сменные. Черчилль назвал тот факт, что англичане научились расшифровывать Энигму, самой большой военной тайной второй мировой войны. В некоторых случаях, даже достоверно зная о немецких операциях (например, о действиях подводных лодок), англичане сознательно отказывались от каких-то контропераций только с целью того, чтобы не дать немцам заподозрить, что они читают немецкие шифротексты. В качестве одного из предположений, которое высказывал советский писатель Пикуль, что благодаря этому подходу был практически погублен полярный канвой ПКУ 17. Хотя, если посмотреть по датам, то в общем не получается - англичане к тому моменту скорее всего ещё не построили дешифровщик, хотя алгоритм был уже понятен.*

*Было известно, что британский командующий Мангомери знал о плане контрнаступления в Арденах, зимой 1944-45 годов. То есть, для союзников это не было никаким секретом.*

Со Второй Мировой закончили.

***Несколько слов о послевоенном развитии.*** Развитие систем передачи данных после войн велось в нескольких направлениях. В первую очередь — это создание всё более устойчивых шифров (если смотреть на криптографию), причём развитие вычислительной техники наконец позволило использовать не только полициклические шифры, но и более стойкие ***полиномиальные шифры***, когда алгоритм основывается не на простой циклической замене, а на более сложных механизмах. И вообще говоря, все современные шифросистемы - это развитие тех или иных полиномиальных шифров. Если их сравнить с полициклическими шифрами-то это одно и то же, что полициклические шифры до Энигмы.

Связано это, во-первых, с очень сложными алгоритмами (например, есть система шифрования, которая построена на конечных преобразованиях Фурье, нота вычислительная сложность на порядки превышает вычислительные сложности полиномиальных алгоритмов).

***Поговорим о передаче данных.*** Развивались механизмы проводной и беспроводной связи.

В первую очередь надо отметить момент, что после войны довольно бурно расцвело такое направление, которое получило название ***аналоговые вычислительные машины*** (авм). Прообразом авм можно считать тот самый британский дешифровщик. Авм во многом были советским ноу-хау. (Почему они на короткое время стали столь популярны, читайте в следующей лекции:)) А вот почему они быстро загнулись, поясним сейчас. Авм — это такая штука, которая позволяла кодировать те или иные математические алгоритмы путём коммутации радиохимических элементов. *Из физики должны были знать:* е*сть три основных электротехнических линейных элемента: сопротивление, конденсатор и индуктивность. Для каждого из них можно написать свой аналог закона Ома для обычного сопротивления. Закон Ома: падение напряжения на этом элементе равно сопротивление умножить на электрический ток, проходящий через этот элемент. Точно так же для конденсатора напряжение — это пропорциональная производная от тока, а для индуктивности - это интеграл.* Эти три простых элемента позволяют закодировать большинство математических алгоритмов, связанных с интегрированием и дифференцированием тех или иных функций. А поскольку большая часть математики оперируется линейными дифференциальными уравнениями, то на основе этих элементов можно собрать такую штуку, которая называется **интегратором.** Т.е. в ней можно закодировать алгоритм решения любого дифференциального уравнения.Для этих целей она и использовалась (для баллистических расчётов в космической военной технике, для расчётов первых атомных реакторов). Пик её применения - это 50ые годы. К 60ым годам все аналоговые устройства были вытеснены цифровыми. Самым большим преимуществом авм было то, что она могла получить результат практически сразу: т. е надо было скоммутировать правильным образом элементы, чтобы они отражали алгоритм решения того или иного диффура (а если мы работаем с линейными диф-ми уравнениями, то там ничего, кроме интегрирования и диф-ия линейных элементов, быть не может). После этого мы подаём на вход некий исходный сигнал (который, например, выражает правую функциональную часть линейного диф-го уравнения). После того, как все релаксационные процессы в электрической сети завершатся, то на выходе получается функция, которая является решением этого диффура. Далее с этой функцией в меру своей фантазии можно делать что угодно (её можно вывести на экран осциллографа, вывести на самописец). Решение, как говорится, у вас в кармане. Все электронные вычислительные машины 1го поколения были чрезвычайно медленными и чрезвычайно не надёжными. А здесь вы получали фактически сразу готовое решение, и если вам это решение чем-то не нравилось, можно было исходную схему поправить, перекоммутировать и попробовать решить с новыми начальными условиями.

К сожалению, у всей аналоговой техники есть очень много серьёзных недостатков. Основным недостатком ЭВМ является то, что линейность там обеспечивается только в первом приближении, т. е даже простейшее сопротивление имеет нелинейные параметры (например, сопротивление меняется от температуры, температура меняется от проходящего тока - по з. Джона Ленца). Чем больше разных элементов, тем больше в схеме накапливается нелинейных искажений. С этим ничего не поделаешь. Любая аналоговая схема имеет параметр, который носит название ***диапазон линейности*** ( - диапазон входных условий, в которых можно рассматривать все элементы этой схемы как линейные). Чем больше в схеме элементов, тем меньше диапазон линейности. Для того чтобы решить задачу при большом количестве исходных значений, придётся построить несколько разных схем, каждая из которых будет соответствовать одному из возможных интервалов исходного диапазона начальных условий. Несмотря на всю кажущуюся простоту, *авм, в конце концов, оказались и не быстрыми и не надёжными и очень сложными в работе и эксплуатации*. Когда цифровые вычислит-е машины перешли на полупроводниковую элементную базу (это случилось во второй половине 50х годов), они перешли по быстродействию авм, и с этого момента у авм начался закат. Тем не менее в СССР в экономических расчётах и в моделировании макроэкономических процессов, где до 60х годов использовались авм. Здесь объяснение очень простое: цифровые авм начали использоваться военными, на народное хоз-во оставалось то, что оставалось.

На самом деле во время войны почти у каждой стороны существовали свои электромеханические шифровалыне машины. Но в СССР пользовались другими методами. У США были. Принцип везде примерно был один и тот же - это множественная электрическая коммутация при помощи перфодиска или при помощи спец. металлических перфокарт (у американцев, например). Вспомним также об Энигме. У неё было ещё одно преимущество: диски содержали множество маленьких проводочков, и когда они соединяют отстоящие друг от друга сегменты диска, они рвутся. Их коммутировали не на диаметрально противоположные сектора диска. Англичане до этого дела не додумались, хотя постфактум, когда в 70е годы все материалы по Энигме были раскрыты, то мировое компьютерное сообщество до этого дела очень быстро додумалось и оказалось, что это тоже можно было использовать (сократить перебор на порядок на два). Понятно, что с перфокартой такого бы не было. ***Американские перфокарты -*** это был лист алюминия (в длину 24 символа, в ширину примерно 6\*24).Этот лист с целью электрического сопротивления покрывался чем-то типа резины, а оставшиеся дырки в нём коммутировали контакты. Там была такая большая матрица 24 на 6 контактов, там, где были в этой перфокарте дырки, они коммутировались. Там также на каждый день должна была быть своя перфокарта.

***Немного про СССР***. Во время всего первого периода Великой Отечественной войны считается, что криптографии в СССР просто не было, по крайней мере, на уровне регулярных частей. Приводило это к известным потерям. На уровне фронтов армии дивизии использовались шифрокниги. Очень большое количество шифрокниг в 41м году было потеряно, что потребовало их восстановления с нуля. Но советские шифрокниги были простыми: там соответствующие фразы кодировались последовательностью из пяти десятичных цифр (пять здесь связано с кодом Бодо). К концу войны получилось довести использование войсковых шифров до полкового уровня. Во всём мире тоже примерно так и было, так что можно сказать, что к концу войны СССР наверстал упущенное. Хоть и известно, что шифромашин в СССР не было, там сидели шифровальщики, но по алгоритмам тоже не всё ясно, что там использовалось. Зато после войны было решено пользоваться совершенно не пробиваемыми шифрами, а именно ***одноразовыми шифроблокнотами.***

Смысл их такой: есть ключ, причём длинный, блокнот - примерно в четверть тетрадного листа размером, на нём написана совершенно случайная последовательность букв, на каждую из них своя собственная последовательность должна использоваться (в идеальном случае вообще однократно). В итоге получилось то же, что с Энигмой - начались повторные использования шифроблокнотов, поэтому часть шифров успешно читалась. Правда, надо отдать должное - в своё время СССР провёл гениальную операцию по дезинформации. То есть, когда стало известно, что американцы из западного Берлина подкопались к советскому кабелю связи штаба западной группы войск с Москвой, после этого по этому кабелю стали гнать исключительную дезу. Причём, американцы об этом так и не узнали, пока этот кабель не вышел из эксплуатации.

***Цифровые машины.*** Они тоже более менее связаны с военным делом. Первую цифровую ЭВМ построили американцы. Это машина, которая получила название ENIAK(Эниак). Построили её в Массачусетском Технологическом институте, она была нужна в рамках Манхэттенского проекта для нейтронно-физических расчетов. Она никаких диффуров считать не умела. Программировали её по средствам коммутационной панели. Для расчётов атомной бомбы надо было просто делать очень много расчётов тупой арифметики (складывать и умножать). Грубо говоря, нужно было составить таблицу сложных функций. Эниак был очень большим (размером с комнату). Она работала на лампах. Потребляла энергии примерно столько, как район целого города, сильно грела воздух. Самое неприятно с Эниаком было то, что раз в 10-15 минут у него выходила из строя очередная электронная лампа. Все цепи у Эниака дублировались и троировались, поэтому она умудрялась пережить один из отказов в цепи по индикации на релейных шкафах. Внутри этих шкафов были триггеры. В одном триггере было две лампы, кучка конденсаторов, кучка сопротивлений. Триггер собирается на электронных триодах. Он умеет запоминать своё собственное состояние. Пока у него идёт входной сигнал, он его переключает на другое. На каждый триггер выводилась на внешнюю панель лампочка: если лампочка горит, значит триггер работает. Основная задача была - смотреть на эти самые панели, смотреть какие лампочки потухли и быстро менять блоки триггеров. Быстродействие в Эниаке было порядка 600-700 операций в секунду.

Более поздние Эниаки программировались при помощи перфокарт. При этом дырочки на перфокарт для контактов пробивались вручную.

***Следующее поколение ЭВМ***-это переход на полупроводниковую технику. В Америке — начало 50х годов, у нас — середина, вторая половина 50х годов. Вместо электронных триодов использовались корпусные транзисторы (один корпус - один транзистор). Разница с лампой по объёму (да и по всем остальным параметрам тоже) на три порядка меньше. Появились первые зачатки нормального программирования. Появилось разделение на процессоры и на периферийные устройства. По вычислительной технике СССР шёл приблизительно вровень со Штатами где-то до второй половины 60х годов. В СССР компьютерная техника развивалась за счёт мощной советской математической школы. У нас были решения, которые в американской технике не использовались или использовались с большим отставанием. Например, в СССР была построена машина на троичной логике. В чём преимущество троичной логики? Там проще реализуется алгоритм целочисленного деления.

*В СССР первой была разработана машина с полной стековой архитектурой.* Называлась она***Эльбрус****.*

В 70е годы сыграла роль одна очень интересная особенность советской вычислительной техники. А именно: после войны советской развитие вычислительной техники было жутко засекречено. В газетах печатались статьи о двух продажных девках империализма: генетике и кибернетике. Причём, на генетику бочку катили всерьёз, а вот с кибернетикой (как выяснилось потом) всё обстояло очень просто. Вся тематике развитие ЭВМ в СССР была жутко засекречена (т.к., в первую очередь, это баллистика и атомная бомба, «чтобы враг не догадался»). Всё в то время вращалось вокруг военной техники, и для обеспечения кадрами этой вычислительной техники хватало спецвузов, их там этому обучали. В связи с тем, что в 60е годы началось массовое производство коммерческих ЭВМ (ЭВМ в интересах народного хоз-ва), стало очень не хватать программистов и операторов. То есть были ЭВМ, не было к ним специфического программного обеспечения. В 70е годы было принято неоднозначное решение о создании советских ЭВМ, унифицированных по программному коду с импортными машинами, чтобы можно было пользоваться контрафактным ПО. *Были созданы две серии машин:* *ЕС ЭВМ и СМ ЭВМ*.

***ЕС ЭВМ*** (ЕС - единая серия). Она была совместима по программному коду с мейнфреймами IBM 360/370.

***СМ ЭВМ***. Была совместима по программному коду с PDP 8 и PDP 11 VAX.

Многие отмечают, что это решение погубило советскую вычислительную технику.

*Во-первых*, эти ЭВМ строились немного на других принципах, чем советские. Те инженеры, которые в СССР занимались разработкой таких машин, как Эльбрус, оказались не удел. Для того чтобы копировать чужие образцы, много ума не надо.

*Во-вторых,* оказались ненужными все собственные советские разработки по алгоритмическим языкам. Стали использоваться языки высокого уровня, которые входили в комплект ПО к этим компьютерам (FORTRAN, ADA).

Появление языка C в своё время очень сильно затормозило развитие алгоритмических языков. Очень многие тенденции 60х годов были напрочь перебиты именно тем, что появился массовый язык, которому можно довольно легко научить. И, что самое главное, стоимость ПО, написанного на языке C, достаточно низка (по причине своей массовости).

В 70е годы уже было понятно, что так или иначе глобальная сеть появится. Вопрос стоял только о том, как она будет выглядеть. В 70е года была высказана мысль (и она продержалась до конца 80х), что глобальная сеть будет чрезвычайно гетерогенной. Там будет дикое количество протоколов физического уровня, сетевого уровня, и будут заметную роль играть хабы (на тот момент - это маршрутизаторы физического уровня, хосты, которые умеют преобразовывать протоколы физического уровня в другой). То, что весь интернет строится на основе протокола IP, такого не ожидал никто. Это была одна из совершенно неожиданных гипотез.

Возвращаясь к советской технике, стоит сказать, что если бы продолжалась советская линейка, то мы бы сейчас не пользовались ноутбуками. У нас бы были свои собственные сети передачи данных и свои собственные протоколы. Отчасти, нам повезло, что СССР очень легко интегрировался в интернет.