Спицына Надежда Александровна, учитель информатики и ИКТ, математики
МБОУ «Школа №127» г. Нижнего Новгорода

Конспект виртуальной экскурсии

Тема экскурсии: «Мир тайнописи и шифрования» (виртуальная экскурсия в историю криптографии).

Целевая аудитория: обучающиеся 6-9 классов.

Цель: способствовать формированию представления о криптографии и многообразии форм шифрования данных.

Задачи:

- вызвать интерес учащихся к проблемам кодирования и декодирования информации в истории человечества и современной жизни;
- расширить представление учащихся о процессе кодирования информации;
- показать закономерности, позволяющие находить ключ к шифрограммам;
- развивать аналитические способности учащихся, путем осуществления шифрования и дешифрования данных с применением изученных методов.

Маршрут экскурсии:

1. **Наука криптография:** основные направления и понятия науки.
2. **Разгадать неразгаданное:** способы шифрования информации в Древней Греции.
3. **Хитросплетение разума:** тайный шифр Юлия Цезаря.
4. **Искусство тайнописи:** история развития и становления криптографии как науки.
5. **Революция в шифровании:** технический прогресс и криптография.
6. **Война кодов и шифров:** важная роль криптографии в истории мировых войн.
7. **Эпилог:** итог экскурсии, заключительное слово.

Спицына Надежда Александровна, учитель информатики и ИКТ, математики
МБОУ «Школа №127» г. Нижнего Новгорода

Структура экскурсии:

Слайд №1 — пролог.

Слайд №2 — титульный.

Слайд №3 — маршрут экскурсии.

Слайды №№4 – 13 — экскурсия.

Слайд №14 — эпилог.

Слайды №№15 – 18 — информационные источники.

Ход экскурсии

№ слайда	Содержание	Навигация, примечания
1. Пролог	*Просмотр пролога.* Тайны и секретные шифры являются неотъемлемой принадлежностью многих детективных романов, в которых действуют изощренные в хитрости шпионы. Писатель-романтик Эдгар По, которого иногда причисляют к создателям детективного жанра, в своем рассказе «Золотой жук» в художественной форме изложил простейшие приемы шифрования и расшифровки сообщений. Шифрованные сообщения встречаются в многих художественных произведениях. Эдгар Аллан По и Конан Дойль, автор знаменитых рассказов о Шерлоке Холмсе, наделили своих героев актуальными умениями разгадывания тайн, и блистательно показали их познания в криптографии — науке, популяризировавшейся во время написания этих произведений.	Музыкальное сопровождение, анимация автоматически, настроена по времени. Переход на следующий слайд осуществляется по управляющей кнопке-стрелке 
2. Титульный	Название экскурсии: «Мир тайн и шифрования» (виртуальная экскурсия в историю криптографии).	Переход на следующий слайд (маршрут экскурсии) осуществляется автоматически.

3. Маршрут экскурсии	*Представление маршрута экскурсии.* Мы познакомимся с самыми тайными и загадочными страницами истории науки. Разгадаем неразгаданное, научимся искусству тайнописи, совершим революцию в шифровании, узнаем, кто же победил в войне кодов и шифров.	Анимация автоматическая. Гиперссылки на объекты маршрута с изображений  замка.
4. Наука криптография	***Тайны сопровождают всю историю человечества***. Без тайн не может быть не только государства, но даже малой общности людей — без них нельзя выиграть сражение или выгодно продать товар, одолеть своих политических противников в жестокой борьбе за власть или сохранить первенство в технологии. Тайны составляют основу науки, техники и политики любой человеческой формации, являясь цементом государственности.	Анимация автоматическая. Переход к следующей информации по щелчку.
	На протяжении последних двух тысяч лет (по крайней мере) всегда находились люди, желающие посылать сообщения, прочитать которые могут лишь те, кому эти сообщения адресованы. Если письмо доставляет получателю посыльный (раб, как это было в Древней Греции или Риме) или современная почтовая служба, всегда есть риск того, что письмо попадет в чужие руки. ***Если есть тайна, то необходимы и способы ее защиты.***	Анимация автоматическая. Переход с следующей информации по щелчку.
	Любое конфиденциальное сообщение может попасть в руки того, кто не должен его видеть. И, следовательно, благоразумно предпринять такие шаги, которые гарантируют, что прочтение этого сообщения окажется для него, по меньшей мере, очень трудным, а лучше всего и вовсе невозможным делом. ***Проблему обеспечения тайны переписки осознавали еще древние греки.***	Анимация автоматическая. Переход к следующей информации по щелчку.
	Греки нашли ***необычное решение: они брили наголо голову раба и писали на ней*** свое ***послание***. ***Когда волосы на голове раба отрастали вновь, его посылали доставить сообщение***. Получатель брил голову раба и прочитывал текст. Ясно, что способ этот очень ненадежен, и вдобавок неэффективен. Всякий, осведомленный о таком способе связи, мог схватить раба, побрить ему голову и прочесть послание. Более того, на отправку сообщения и получения ответа таким способом уходило несколько недель.	Анимация автоматическая. Переход к следующей информации по щелчку.
	Политики и военные, священники и торговцы, писатели и ученые, шарлатаны и аферисты тысячелетиями развивали приемы защиты секретов***. Со временем способы сокрытия информации совершенствовались, и тайнопись выделилась в отдельную науку — науку криптографию***.	Анимация автоматическая. Переход на следующий слайд по щелчку.

5. Наука криптография	**Криптография (*тайнопись*) *(от древнегреческого κρυπτός — скрытый и γράφω — пишу) — наука о способах обеспечения секретности сообщения.*** Это — одна из старейших наук, ее история насчитывает несколько тысяч лет. Криптография позволяет хранить важную информацию или передавать ее по ненадежным каналам связи.	Анимация автоматическая. Переход к следующей информации по управляющей кнопке.
	Термин криптография ввел выдающийся английский математик XVII века Джон Валлис (1616-1703) — английский математик, один из основателей и первых членов Лондонского королевского общества. Профессор геометрии Оксфордского университета. Примечательно, что Валлис никакого математического образования не получал, а занимался самостоятельно. Сын священника из Эшфорда уже в молодости вызывал восхищение как *феноменальный счётчик*: как-то в уме извлёк квадратный корень из 53-значного числа. Он изучал криптографию, и применял свои знания к расшифровке различного рода политической переписки при дворе короля Карла II.	Анимация автоматическая. Переход к следующей информации по управляющей кнопке.
	Сообщение всегда может попасть в руки огромному числу лиц, которым оно не предназначается. Если информация написана ***открытым текстом***, то есть, выражаясь обычным языком, не сделано никаких попыток скрыть его содержание, то любой, к кому оно попадет, сможет прочесть его и понять, если он знает язык, на котором оно написано.	Анимация автоматическая. Переход к следующей информации по управляющей кнопке.
	Цель криптографии состоит в том, чтобы скрыть смысл сообщения, — процесс известный как шифрование. Чтобы сделать сообщение непонятным (***шифрованное сообщение***), оно зашифровывается по определенному правилу, которое заранее обговаривается между отправителем сообщения и его получателем. Преимущество криптографии состоит в том, что если противник перехватит зашифрованное сообщение, то прочитать его ему не удастся. Восстановить исходное сообщение, не зная правила шифрования, может оказаться для противника сложной, а то и вообще невыполнимой задачей.	Анимация автоматическая. Переход к следующей информации по управляющей кнопке.
	Чтобы зашифровать исходный текст сообщения отправитель применяет к нему алгоритм шифрования. ***Шифр — какая-либо система преобразования текста с секретом (ключом)***. Получатель, который знает и ключ, и алгоритм, использованные отправителем, сможет преобразовать зашифрованный текст сообщения обратно в исходный вид.	Анимация автоматическая. Щелчок по слову «**ШИФР»** вызывает макрос: диалоговое окно — определение понятия.
	Возврат на маршрутный лист.	Возврат на маршрутный лист по управляющей кнопке (лупа).

6. Разгадать неразгаданное	Шифрование появилось в глубокой древности. Уже знаменитый греческий историк Геродот (V век до н.э.) приводил примеры писем, понятных лишь для одного адресата. ***Хрестоматийным является пример криптографии в Древней Греции, относящийся к V в. до н. э.*** Спартанцы имели специальный механический прибор, при помощи которого важные сообщения можно было писать особым способом, обеспечивающим сохранение тайны.	Анимация автоматическая. Переход к следующей информации по щелчку.
	Во время войны Спарты против Афин для передачи военных донесений использовался так называемый шифр «Сцитала» (или скитала).	Переход к следующей информации по щелчку.
	«Сцитала» представляла собой цилиндрический жезл, на который наматывалась узкая полоска папируса, пергамента или кожи. Отправитель писал сообщение по всей длине сциталы, а затем разматывал полоску, на которой после этого оставался бессмысленный набор букв. Сообщение оказывалось зашифрованным.	Переход к следующей информации по щелчку.
	После этого полоска папируса с текстом посылалась адресату, имеющему точно такой же стержень, что позволяло ему прочитать сообщение. Чтобы получить исходное сообщение адресат просто наматывал полоску вокруг стержня, того же диаметра, что и пользовался отправитель. В 404 году до н.э. к спартанскому полководцу Лисандру привели вестника, окровавленного и еле державшегося на ногах, одного из пяти оставшихся в живых после крайне опасного путешествия из Персии. Вестник передал свой пояс Лисандру, который намотал его вокруг своей скиталы и прочитал, что Фарнабаз (персидский сатрап и военачальник) собирается напасть на него. Благодаря скитале Лисандр успел подготовится к нападению и отбил его.	Переход к следующей информации по щелчку (появляется изображение письма).
	Тайное письмо. ***На наш адрес поступило зашифрованное сообщение. Укажите, как, пользуясь имеющимися данными, прочитать текст.*** Ребятам выдается раздаточный материал (**Приложение №1. Шифр «сцитала»**). Ребята отгадывают тайное сообщение. Ответ записывают в карточку, и сдают учителю. Учитель проверяет, выполнение задания, зачисляет баллы для каждой группы. Правильные ответы: **№1.** ЧТО ОДНОМУ С ТРУДОМ ДАЕТСЯ, ТО КОЛЛЕКТИВОМ ЛЕГКО БЕРЕТСЯ. **№2**. ЧТО ОДНОМУ НЕСРУЧНО, ТО КОЛЛЕКТИВУ СПОДРУЧНО. **№3.** ЧТО ОДНОМУ НЕ ПОД СИЛУ, ТО ЛЕГКО КОЛЛЕКТИВУ. **№4**. ХОРОШАЯ НИВА ТОЛЬКО У КОЛЛЕКТИВА.	Щелчок по изображению вызывает макрос: диалоговое окно — задание. Групповая работа **(Приложение №1).**  Переход к следующей информации по щелчку.

	В спартанской сцитале был реализован один из способов перестановки. Перестановка одно из двух направлений криптографии. ***При перестановке буквы сообщения меняют свое местоположение, образуя анаграмму.*** Для очень короткого сообщения, состоящего, например, из одного слова, такой способ весьма ненадежен, поскольку существует крайне ограниченное число возможных способов перестановки горстки букв.	
	Попробуйте составить число всевозможных перестановок из трех букв **И, К** и **Т. Сколько способов у вас получилось?** Действительно, три буквы могут быть расставлены всего лишь шестью различными способами: ИКТ, ИТК, КИТ, КТИ, ТИК, ТКИ.	Индивидуальная работа. Появление правильного ответа (6 способов) по щелчку. Переход к следующей информации по щелчку.
	Однако, по мере увеличения количества букв, число возможных перестановок стремительно растет, и восстановить исходное сообщение становится невозможным, если не известен точный способ шифрования. **НАПРИМЕР, ЭТО КОРОТКОЕ ПРЕДЛОЖЕНИЕ.** В этом предложении содержится 35 символов, а число их различных перестановок составляет более 50.000.000.000.000.000.000.000.000.000.000 способов.	Переход к следующей информации по щелчку.
	Если бы все люди на Земле работали день и ночь, чтобы проверить все перестановки, потребовалось бы времени в тысячи раз больше, чем срок существования Вселенной.	Анимация автоматическая. Переход на следующий слайд по щелчку.
7. Разгадать неразгаданное	***Древнегреческий полководец IV века до н.э. Эней Тактик в своем сочинении «О перенесении осады» описал еще одну технику тайнописи*** – так называемый книжный шифр Энея.	Анимация автоматическая. Переход к следующей информации по управляющей кнопке.
	Он предложил делать дырки рядом с буквами в книге или другом документе. Малозаметные пометки в тексте, например игольные дырки, в сумме образовывали исходный текст секретного сообщения.	Переход к следующей информации по управляющей кнопке.
	Много позже аналогичный шифр использовали германские шпионы в Первой мировой войне.	Переход к следующей информации по управляющей кнопке.

	Одна из древнейших систем кодирования предложена греческим историком, полководцем, государственным деятелем Полибием (II век до н.э.). Данный вид кодирования изначально применялся для греческого алфавита, но затем был распространен на другие языки.	Переход к следующей информации по управляющей кнопке. 
	Для шифрования, прежде всего, необходимо составить таблицу, куда нужно вписать все буквы используемого алфавита. Нередко в таблице использовался именно алфавитный порядок расположения букв. Пример: ***«Квадрат Полибия» представляет собой квадрат 5х5, столбцы и строки которого нумеруются цифрами от 1 до 5. В каждую клетку этого квадрата записывается одна буква.*** В результате, каждой букве соответствует пара чисел, и шифрованное сообщение превращается в последовательность пар чисел. Расшифровывается путем нахождения буквы, стоящей на пересечении строки и столбца.	Переход к следующей информации по управляющей кнопке. 
	Тайное письмо. ***На наш адрес поступило зашифрованное сообщение. Укажите, как, пользуясь имеющимися данными, прочитать текст.*** Ребятам выдается раздаточный материал (**Приложение №2.Квадрат Полибия.**). Ребята отгадывают тайное сообщение. Ответ записывают в карточку, и сдают учителю. Учитель проверяет, выполнение задания, зачисляет баллы для каждой группы. Правильные ответы: №1. ВОДА У ДРУГА ЛУЧШЕ, ЧЕМ У ВРАГА МЁД. №2. ДЛЯ ДОРОГОГО ДРУГА – ВОРОТА НАСТЕЖ, №3. ЧЕЛОВЕК БЕЗ ДРУГА, ЧТО ЗЕМЛЯ БЕЗ ВОДЫ. №4. ЧЕЛОВЕК БЕЗ ДРУЗЕЙ, ЧТО СОКОЛ БЕЗ КРЫЛЬЕВ,	Щелчок по изображению вызывает макрос: диалоговое окно — задание. Групповая работа. **(Приложение №2).** 
	Возврат на маршрутный лист.	Возврат на маршрутный лист по управляющей кнопке (лупа). 
8. Хитросплетение разума	Поднимаются ворота. Шифрованная связь для римских органов власти была жизненно необходимой. Документальное подтверждение использования шифрования информации в военных целях появилось в «Галльских войнах» Юлия Цезаря. Цезарь описывает как он послал сообщение Цицерону, находящемуся в осаде и бывшему на грани капитуляции. В этом письме латинские буквы были заменены греческими, поэтому враг его не смог бы понять. Цезарь описал драматичность доставки письма:	Анимация поднятия ворот по щелчку. Следующая анимация автоматически. Учитель зачитывает письмо Цезаря **(Приложение №5).**

	Гонцу дали наставление, что если он не сможет приблизится, то должен метнуть дротик с прикрепленным к ремешку письмом так, чтобы оно упало в лагере. Убоявшись излишнего риска, галльский всадник метнул дротик, как ему приказали. По случайности дротик попал в башню, и в течение двух дней наши отряды его не замечали; только на третий день его увидел солдат, вытащил и доставил Цицерону. Цицерон просмотрел письмо, а затем прочитал его на собрании солдат, что вызвало у всех огромную радость.	Переход к следующей информации по щелчку.
	Цезарь часто пользовался тайнописью. ***Не доверяя гонцам, Юлий Цезарь шифровал свои депеши, используя способ, который получил название «Шифр Цезаря».*** Дошел он до нас благодаря сочинению Гая Транквилла Светония «Жизнь 12 Цезарей», написанному во II веке н.э.	Переход к следующей информации по щелчку.
	Каждую букву сообщения он заменял на другую, которая в латинском алфавите отстояла от исходной на три позиции дальше. Таким образом, буква A латинского алфавита заменялась на D, B на E, и так далее вплоть до буквы W, которая заменялась на Z, затем X на A, Y на B и, наконец, Z на C. Криптографы часто пользуются терминами: *алфавит открытого текста*, то есть алфавит, используемый для создания незашифрованного сообщения, и *шифралфавит*, буквы которого подставляются вместо букв открытого текста. Если алфавит открытого текста расположить над шифралфавитом, то станет ясно, что ***в шифре Цезаря каждая буква алфавита циклически сдвигается на 3 позиции.***	Переход к следующей информации по щелчку.
	Если бы он проделал это со своим знаменитым ***посланием сенату, сделанное после однодневной войны с понтийским царем Фарнаком*** **VENI.VIDI.VICI (ПРИШЕЛ, УВИДЕЛ, ПОБЕДИЛ)**, то отправленное сообщение выглядело бы так: **SBKF SFAF SFZF**.	Переход на следующий слайд по щелчку.
9. Хитросплетение разума	***Позже, в XV веке, итальянский ученый***, флорентийский энциклопедист ***Леон Батиста Альберти*** предложил использовать два и более шифралфавитов, и ***создал шифровальный диск***, с помощью которого легко можно было шифровать сообщения, переходя от одного шифралфавита к другому, сбивая с толку возможных противников. Несмотря на то, что Альберти совершил самый значительный, за более чем тысячу лет, переворот в криптографии, он не сумел довести свою идею до целостной системы.	Анимация автоматическая. Переход к следующей информации по управляющей кнопке. 

	Решать эту задачу предстояло другим: Иоганну Тритемию (немецкому аббату), Джованни Порта (итальянскому ученому), и, наконец Блезу де Виженеру, ***В XVI веке французский дипломат Блез Виженер усложнил шифр. «Шифр Виженера» долгое время считался самым стойким к взлому***, но и трудным для самих шифровальщиков.	Анимация автоматическая. Переход к следующей информации по управляющей кнопке. 
	«Шифр Цезаря» — не очень сложный метод, тем не менее, Цезарь вошел в историю криптографии, а его способ шифрования до сих пор служит примером одной из первых систем шифрования и является частным случаем шифра простой замены. Метод замены: каждая буква в исходном тексте заменяется другой буквой.	Анимация автоматическая. Переход к следующей информации по управляющей кнопке. 
	Если использовать алфавит с 26 буквами, то можно осуществить сдвиг на 1..25 позиций, то есть мы получим 25 различных шифров.	Анимация автоматическая. Переход к следующей информации по управляющей кнопке. 
	Если добавить еще перестановки, то получится свыше **400 000 000 000 000 000 000 000 000** возможных способов шифрования информации.	Анимация автоматическая. Переход к следующей информации по управляющей кнопке. 
	Тайное письмо. ***На наш адрес поступило зашифрованное сообщение. Укажите, как, пользуясь имеющимися данными, прочитать текст.*** Ребятам выдается раздаточный материал (**Приложение №3. Шифр Цезаря.**). Ребята зашифровывают сообщение с помощью шифровального круга, передают сообщение другой группе, которые, в свою очередь, дешифруют сообщение. Ребята отгадывают тайное сообщение. Ответ записывают в карточку, и сдают учителю. Учитель проверяет, выполнение задания, зачисляет баллы для каждой группы. Правильные ответы: №1. ЛЕНЬ ДОБРА НЕ ДЕЕТ. №2. ДОБРА НА ХУДО НЕ МЕНЯЮТ. №3. ДОБРО И ВО СНЕ ХОРОШО. №4. ДОБРО ХУДО ПЕРЕМНОЖИТ.	Щелчок по изображению вызывает макрос: диалоговое окно — задание. Групповая работа. **(Приложение №3).** 

	Возврат на маршрутный лист.	Возврат на маршрутный лист по управляющей кнопке (лупа). 
10. Искусство тайнописи	Появление главных героев фильма «Приключения Шерлока Холмса и доктора Ватсона. Звучит речь Ватсона и Холмса: «— Так, какие-то иероглифы... — Прекрасно, Ватсон. Впереди расшифровка!»	Анимация автоматическая. Звук воспроизводится автоматически. Переход к следующей информации по щелчку.
	Раскрывается книга. Точных дат и достоверных данных о тайнописи в древности никто не приводит.	Появление книги – анимация автоматическая. Листание следующей страницы по щелчку.
	Интересно, что ***в глубокой древности тайнопись считалась одним из 64-х искусств, которым следует владеть как мужчинам, так и женщинам. Сведения о способах шифрованного письма можно обнаружить уже в документах древних цивилизаций Индии, Египта, Месопотамии.*** Словом, к началу нашей эры люди знали о криптографии довольно много и использовали ее достаточно широко. Последующие 19 веков были потрачены на изобретение более или менее хитроумных способов шифрования.	Листание следующей страницы по щелчку.
	Период расцвета арабских государств (VIII век н. э.) — поистине эпоха великих открытий в области криптографии. Не зря ведь слово «шифр», как и слово «цифра», имеет арабские корни. ***В появившейся в 855 году арабской «Книге о стремлении человека разгадать загадки древней письменности» описываются различные системы защиты информации***, в том числе и несколько классических шифралфавитов. Один такой шифралфавит, называвшийся «дауди» (по имени израильского царя Давида), использовался для шифрования трактатов по черной магии. Он был составлен из видоизмененных букв древнееврейского алфавита.	Листание следующей страницы по щелчку.
	В это время Европа прочно увязла в Темных веках: черная магия и криптография в сознании людей были крепко связаны.	Листание следующей страницы по щелчку.

	Иного и быть не могло, ведь ***тайнопись в Европе изначально использовали для того, чтобы скрыть от любопытных глаз содержание документов, описывающих колдовские рецепты, заговоры, гадания и заклинания.*** Алхимики засекречивали с помощью шифров формулы философского камня. В результате, как заклинания и магические формулы вроде «абракадабры», так и зашифрованные письма походили с виду на чепуху, но в действительности имели глубокий смысл.	
	Широкое развитие торговли в средние века потребовало использование шифров торговцами, купцами и даже простыми людьми.	Листание следующей страницы по щелчку.
	Применявшиеся шифрсистемы были предельно просты — фразы писались по вертикали или в обратном порядке, гласные пропускались или заменялись точками, использовались иностранные алфавиты (например, древнееврейский и армянский), каждая буква открытого текста заменялась следовавшей за ней буквой, ***цифра на букву***. Собственно, это **коды,** а не шифры. ***Код – правило (алгоритм) сопоставления конкретному сообщению строго определенной комбинации символов. Например, обозначение даты приготовления на банках консервов.***	Щелчок по слову «**коды»** вызывает макрос: диалоговое окно — определение понятия.
	К XV веку европейская криптография превращается в целую отрасль, развивающуюся стремительными темпами. В эпоху Возрождения, в пору буйного расцвета наук и ремесел в итальянских городах-государствах, шифры стали широко применяться учеными для защиты приоритета научных открытий. В 1466 году в папскую канцелярию представляется трактат о шифрах Леона Альберти, где предлагается собственный шифр с нескромным названием «шифр королей». В начале XVI века Маттео Арженти, криптограф папской канцелярии, изобрел код, согласно которому могут заменяться не только буквы, но и слоги, слова, даже целые фразы, появляется и числовой код. Примерно в то же время, французский посол в Риме Блез Виженер, познакомившись с трудами по криптографии, пишет книгу «Трактат о шифрах» (1585 г.). Его мысль о том, что «Вся природа является просто шифром и секретным письмом», позднее повторят и Блез Паскаль, и отец кибернетики Норберт Винер.	Листание следующей страницы по щелчку.
	В XVI веке криптография превратилась в важный фактор военных отношений, широко использовалась европейскими правителями. Пользовалась шифрованием своих писем и Мария Стюарт, королева Шотландии, когда находилась в заключении в Англии.	Листание следующей страницы по щелчку.

	Каждое письмо перехватывалось, аккуратно вскрывалось, копировалось и расшифровалось Томасом Фелиппесом, специалистом по подделке почерка и шифровальщиком. Затем их отправляли адресатам, которые, естественно, ничего не подозревали. Из этих писем и стали известны детали так называемого Бабингтонского заговора. Бабингтон просил у Марии одобрения на убийство Елизаветы I. Это и предрешило ее судьбу. Марию Стюарт обезглавили.	
	Появляются первые дипломатические и криптографические службы в странах Европы и России. В России, хотя тайнопись использовалась уже в XII–XIII веках, официальной датой появления криптографической службы считается 1549 год (царствование Ивана IV), а именно образование «посольского приказа», при котором имелось «цифирное отделение». Шифры использовались такие же, как на западе — значковые, замены, перестановки. Петр I позднее полностью реорганизовал криптографическую службу, создав Посольскую канцелярию. В это время появляются специальные коды для шифрования — «цифирные азбуки». Все заметнее переход криптографии из области черной магии в область чистой математики. Мы почти ничего не знаем о том, занимались ли ведущие математики того времени проблемами шифрования и дешифрования, но есть данные, что некоторые из них владели криптографией, ***Многие выдающиеся математики стали привлекаться к криптографической службе, среди них Леонард Эйлер и Франсуа Виет.***	Листание следующей страницы по щелчку.
	XVII век — эра «черных кабинетов» - специальных государственных органов по перехвату и дешифровке сообщений, в которых работали криптоаналитики. В Англии Оливер Кромвель создает «Интеллидженс сервис», в состав которой входит подразделение по дешифровке. Не отстает и Франция. Там дешифровальное отделение было создано при Людовике XIV по предложению кардинала Ришелье. В России «черные кабинеты» действовали со времен правления императрицы Елизаветы. Так же, как в Англии и Австрии, они размещались в почтовых отделениях. В число их сотрудников входили специалисты по вскрытию конвертов и подделке печатей, переводчики и дешифровальщики. ***К XVIII веку криптография окончательно складывается как научная дисциплина. Появились системы обучения, значительное количество работ по криптографии и криптоанализу***. ***Криптоанализ — наука о методах расшифровки зашифрованной информации без ключа.*** Становится все более понятно, что защита информации — не столько искусство сочинения и отгадывания изощренных шифров, сколько точная наука.	Щелчок по слову «**криптоанализу»** вызывает макрос: диалоговое окно — определение понятия. Переход на следующий слайд по щелчку.

11. Искусство тайнописи	Перед вами портреты трех великих людей: ⁜ ***Фрэнсис Бэкон*** —английский философ, историк, политический деятель; ⁜ ***Кардинал Ришелье*** (прозвище «Красный герцог) — кардинал Римско-католической церкви, аристократ и государственный деятель Франции; ⁜ ***Александр Сергеевич Грибоедов*** — русский дипломат, поэт, драматург, пианист и композитор, статский советник. ***Как вы думаете, что объединяет этих людей?***	Анимация автоматическая. Переход к следующей информации по управляющей кнопке-стрелке.
	Все они использовали в личной и деловой переписке «решетку Кардано». ***В 1550 году, Джерламо Кардано*** — итальянский математик, инженер, философ, медик и астролог, ***предложил простую решетку для шифрования сообщений.*** Он планировал маскировать сообщения под обычное послание, так что, в целом, они не были полностью похожи на шифрованные. Решетка содержит отверстия для отдельных символов, а сообщение заполняется набором букв или цифр, и представляет собой криптограмму.	Переход к следующей информации по управляющей кнопке-стрелке.
	В 1828 году должность российского представителя в Персии занимал известный русский писатель, общественный деятель и дипломат Александр Сергеевич Грибоедов. Он использовал в своих письмах шифр, известный как "решетка Кардано". ***Грибоедов писал своей жене «невинные послания», с которыми знакомились сотрудники МИД. Они расшифровывали сообщения и затем доставляли письма адресату. Жена, видимо, и не догадывалась о двойном назначении этих посланий.*** Уже в советское время некоторых биографов Грибоедова смутил тот факт, что в отдельных письмах из Персии нарушался характерный стиль знаменитого писателя. При исследовании оказалось, что эти письма содержали дипломатические послания Александра Сергеевича. Раскрыли эту систему очень просто. Сложили все листочки в стопку и просветили мощной лампой. Буквы, стоявшие на местах окон решетки, давали темные пятна, так как лежали строго друг под другом. По этим пятнам легко восстанавливалась решетка, то есть ключ.	Переход к следующей информации по управляющей кнопке-стрелке.
	Одна из разновидностей решетки Кардано — вращающаяся решетка или сетка, в основе которой лежит шахматная доска, которая использовалась в конце XVI века.	Анимация появления объектов автоматическая.

	Для расшифровки сообщения надо: приложить решетку к зашифрованному сообщению, выписать буквы, которые появились в открытых ячейках, повернуть решетку по часовой стрелке на 90^0 (используют и другие виды движения – повороты, симметрию), выписать вновь появившиеся буквы и т.д., пока не расшифруется сообщение полностью. Пример на слайде. Зашифрованное сообщение: ВЕК ЖИВИ — ВЕК УЧИСЬ.	Пример: анимация движения решетки и появления ответа осуществляется по изображению кнопки (триггер). Появление конверта-задания осуществляется по изображению кнопки (триггер).  
	Тайное письмо. ***На наш адрес поступило зашифрованное сообщение. Укажите, как, пользуясь имеющимися данными, прочитать текст.*** Ребятам выдается раздаточный материал (**Приложение №4. Решетка Кардано.**). Ребята отгадывают тайное сообщение. Ответ записывают в карточку, и сдают учителю. Учитель проверяет, выполнение задания, зачисляет баллы для каждой группы. Правильные ответы: №1. БЕЗ МУКИ НЕТ НАУКИ. №2. НА ОШИБКАХ УЧАТСЯ. №3. НЕ ПЕРОМ ПИШУТ — УМОМ. №4. ОТ УЧИТЕЛЯ И НАУКА.	Щелчок по изображению конверта (триггер)  вызывает макрос: диалоговое окно — задание. Групповая работа. **(Приложение №4).**
	Возврат на маршрутный лист.	Возврат на маршрутный лист по управляющей кнопке (лупа). 
12. Революция в шифровании	В XVIII веке становится понятно, что защита информации не столько искусство сочинения и отгадывания изощренных шифров, сколько точная наука.	Анимация автоматическая. Переход к следующей информации по управляющей кнопке-стрелке. 

	Великие ученые разрабатывают и создают новые теории в области математики, физики. Среди них ***Блез Паскаль***, сделавший ряд открытий в области комбинаторики, и создавший метод индуктивного доказательства***; Исаак Ньютон*** и ***Готфрид Лейбниц***, разработавшие дифференциальное и интегральное исчисление. Свои обширные исследования они применяют и в области криптографии.	Переход к следующей информации по управляющей кнопке-стрелке. 
	В начале XIX века криптография обогатилась замечательным изобретением. Его автор — государственный деятель, первый государственный секретарь, а затем и президент США Томас Джефферсон. Это устройство состоит из набора одинаковых пронумерованных дисков, смонтированных на одной оси, причем каждый диск можно вращать независимо. По кромке дисков, в некотором случайном порядке (вообще говоря, разном для каждого диска), нанесены буквы алфавита. Это изобретение стало предвестником появления, так называемых, дисковых шифраторов, нашедших широкое распространение в развитых странах в XX веке.	Переход к следующей информации по управляющей кнопке-стрелке. 
	XIX век ознаменовался революционными изменениями: средствами передачи информации. На рубеже веков связь перестает быть исключительно почтовой, она становится электрической: появляется телеграф, а затем и радио. Это преобразило и криптографию, поскольку возможности доступа противника к шифрованному тексту расширились, появились возможности влиять на открытый текст. Вслед за изменением связи меняется и криптография, становясь сначала электромеханической, а затем электронной.	Переход к следующей информации по управляющей кнопке-стрелке. 
	В 1883 году криптография получила новые идеи, изложенные в ***труде под названием «Военная криптография»***. Интересно, что его ***автор, Огюст Кергоффс***, не был ни военным, ни профессиональным шифровальщиком, зато он преподавал иностранные языки и математику. Опираясь на знания в области лингвистики и математики, автор проводит сравнительный анализ шифров, на основе которого формулирует требования к шифрам и делает вывод, что практический интерес представляют только те шифры, которые остаются стойкими даже при интенсивной переписке.	Переход к следующей информации по управляющей кнопке-стрелке. 
	Благодаря работам Кергоффса, во всем мире криптографию признают наукой, и в обязательном порядке начинают преподавать в военных академиях.	

	Можно считать, что именно Кергоффс написал основы современной криптографии, один из главных принципов которой гласит, что стойкость криптографической системы зависит не от процесса шифрования, а от используемого ключа. Этот принцип не потерял своей актуальности и сегодня.	
	Возврат на маршрутный лист.	Возврат на маршрутный лист по управляющей кнопке (лупа). 
13. Война кодов и шифров	***XX век — век двух мировых войн, век научно-технического прогресса, век социальных потрясений и передела государственных границ.*** Во время Первой мировой войны главным (и зачастую единственным) средством шифрования были коды. Несмотря на то, что все участники боевых действий постоянно разрабатывали новые коды и улучшали старые, обеспечить их сохранность удавалось далеко не всегда, поэтому противники нередко были полностью осведомлены обо всем, что содержалось в секретной переписке врага.	Анимация автоматическая. Переход к следующей информации по управляющей кнопке. 
	Война и радиосвязь полностью преобразили криптографию. Шифрованный текст, переданный по радио, был доступен каждому, кто имел в своем распоряжении несложный приемник. И даже если этот текст нельзя было расшифровать сразу, — его можно использовать при анализе последующих сообщений. ***В этот период получили развитие методы дешифрования, основанные на переборе вероятных ключей.***	Переход к следующей информации по управляющей кнопке. 
	Криптография изучает построение и использование систем шифрования, их стойкость, слабости и степень уязвимости. ***Криптоанализ*** изучает методы вскрытия систем шифрования. Это два направления ***криптоло□гии — науки, занимающейся методами шифрования и дешифрования.*** Криптографы и криптоаналитики - соперники; они стремятся перехитрить друг друга. Каждый ставит себя на место противника и задет себе вопрос: "Если бы я был на его месте, что бы я сделал, чтобы оказаться победителем?". Оба соперника, которые наверняка никогда не встретятся, вовлечены в захватывающий интеллектуальный поединок, в котором ставки могут быть чрезвычайно высоки.	Переход к следующей информации по управляющей кнопке. 

	Это война между создателями шифров и теми, кто их взламывает, интеллектуальная гонка вооружений, которая оказала разительное влияние на ход истории.	Включение видео по управляющей кнопке.  Длительность видеофрагмента 3:47
	*Видео о широко известной шифрмашине «**Энигма**», которой были оснащены германские войска времен Второй мировой войны, и взломе ее кода с помощью «бомбы» Алана Тьюринга.*	
	Возврат на маршрутный лист.	Возврат на маршрутный лист по управляющей кнопке (изображение лупы). 
14. Эпилог	Роль шифров в истории огромна. Шифры решали результаты сражений и приводили к смерти королей и королев. Но шифры сегодня имеют гораздо большее значение, чем когда бы то ни было раньше. Поскольку информация становится все более и более ценным товаром, а революция в сфере коммуникаций изменяет общество. ***Все мы сегодня, иногда даже не подозревая об этом, применяем средства защиты информации:*** ➢ ***шифруем сообщения электронной почты;*** ➢ ***пользуемся интеллектуальными банковскими карточками;*** ➢ ***ведем разговоры по закрытым каналам связи и т. д.***	Анимация автоматическая. Переход к следующей информации по щелчку.
	Всякий раз возникает вопрос — надежна ли защита?	Переход к следующей информации по щелчку
	Над решением проблем защиты информации и работает современная криптография.	Анимация автоматическая. Выход из презентации по управляющей кнопке. 
	Подведение итогов. Выставление оценок. Запись домашнего задания. *Домашнее задание: придумать (красиво оформить в виде буклета) свой уникальный способ шифрования информации, показать применение на 2-3 примерах.*	