1999

БелКрипто: 20+

1 Алиса

Алиса и Боб – известные участники криптографических протоколов. Они появляются даже в серьезных научных статьях по криптографии. Первое появление – 1978 год, знаменитая работа Ривеста, Шамира и Адлемана с описанием криптосистемы RSA: “For our scenarios we suppose that A and B (also known as Alice and Bob) are two users of a public-key cryptosystem”. Выбор имени Алиса несомненно инспирирован сказками Льюиса Кэролла “Приключения Алисы в Стране чудес” и “Алиса в Зазеркалье”, экранизированными огромное число раз.

А в каком из следующих фильмов не было персонажа с именем Алиса?

A Гостья из будущего.

B Приключения Буратино.

C Матрица.

D Последний из могикан.

30:00

Start

2 Боб

Это изобретение 1995 года, названное Bob, получило 7-е место в списке «25 худших продуктов всех времен» журнала PC World, вошло в список «50 худших изобретений» Time Magazine и заняло 1-е место в списке худших продуктов десятилетия CNET.com. О чем речь?

A Гироскутер.

B Графический интерфейс пользователя.

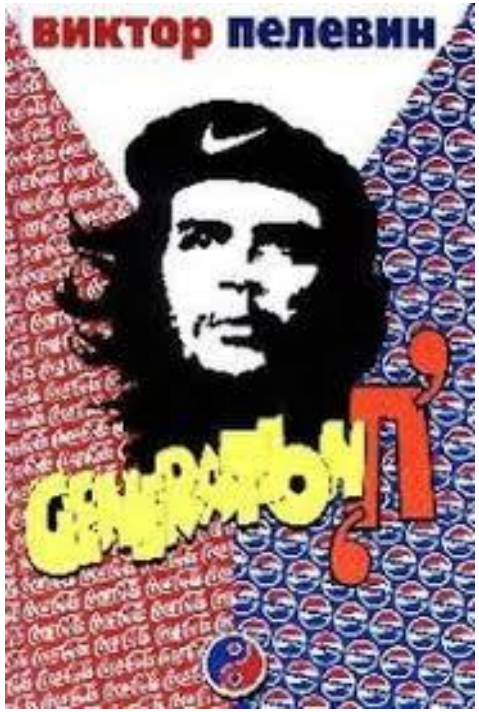
C Очки с электронной регулировкой.

D Бумбокс с дистанционным управлением.

30:00

Start

3 Generation П



В 1999 году вышел в свет культовый роман Виктора Пелевина “Generation П”. В одном из эпизодов главный герой поднимается на недостроенное здание на заброшенной стройке (зиккурат) и находит три предмета. Какой предмет из следующего списка лишний?

A Пачка из-под сигарет «Парламент» с изображением трех пальм.

B USB-флешка с записями речи Че Гевары, полинезийской песни и тантрической мантры.

C Кубинская монета в три песо.

D Пластиковая точилка для карандашей в виде телевизора.

30:00

Start

4 Простое

$$2^{82589933} - 1$$

Стандарт ЭЦП СТБ 1176.2 был принят в 1999 году. Но еще раньше, в 1997, были стандартизированы три протокола формирования общего ключа в стиле Диффи–Хеллмана. Протоколы были введены в форме Проекта руководящего документа Республики Беларусь (сначала Национального Банка) “Протоколы формирования общего ключа”. К сожалению, Проект РД РБ так и остался проектом.

И в СТБ 1176.2, и в Проекте РД РБ широко используются простые числа. Они нужны, чтобы заработала базовая математика. А для того, чтобы обеспечить криптографическую стойкость, простые числа должны иметь внушительную битовую длину.

Число

p = 98A3DF52 AEAE9799 325CB258 D767EBD1 F4630E9B 9E21732A 4AFB1624 BA6DF911 466AD8DA 960586F4 A0D5E3C3 6AF09966 0BDDC157 7E54A9F4 02334433 ACB14BCB (шестнадцатеричная запись, 512 битов)

является простым. А чем еще оно интересно?

A Является простым Ферма.

B Является простым Мерсенна.

C Рекомендовано для использования в СТБ 1176.2.

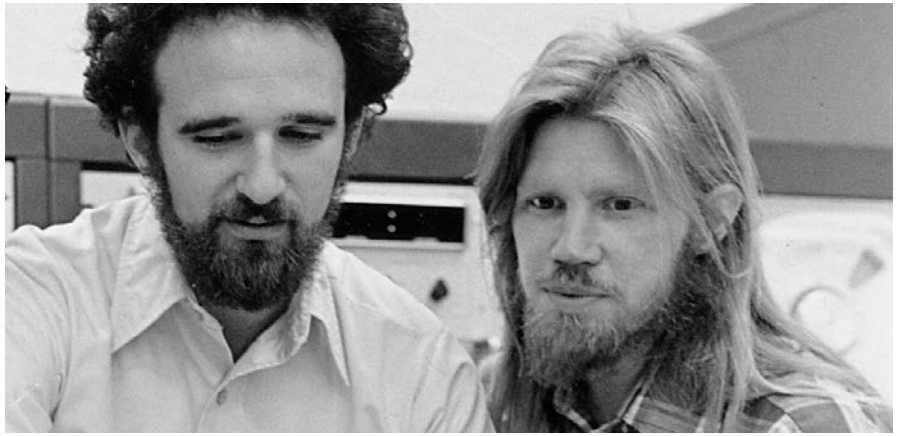
D Рекомендовано для использования в Проекте РД РБ.

E Запатентовано.

30:00

Start

5 Диффи и Хеллман



У. Диффи и М. Хеллман – американские криптографы, работа которых “Новые направления в криптографии” вышла в свет в 1976 году. В этой работе фактически впервые в открытой печати была представлена концепция криптографии с открытым ключом. Концепция была проиллюстрирована протоколом формирования общего ключа (ПФОК), названным впоследствии протоколом Диффи – Хеллмана. Этот протокол является криптографической основной защищенного онлайн-взаимодействия. Всякий раз, открывая HTTPS-соединение, вы, скорее всего, используете какую либо из многочисленных модификаций протокола.

Хеллмана звали Мартин. А как звали Диффи?

A Уилфилд.

B Уилфрид.

C Уитфилд.

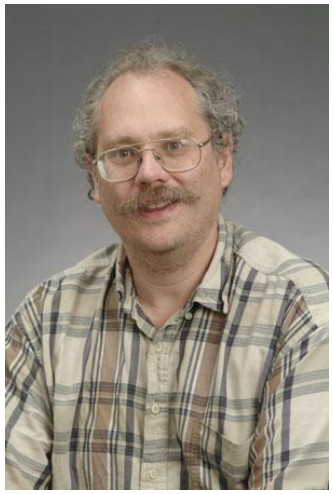
D Уитфрид.

E Уинфилд.

30:00

Start

6 Шнорр или Шор



В 1990 году немецкий математик Клаусом Шнорром предложил схему ЭЦП, которая стала чрезвычайно популярной и, в частности, была использована в СТБ 1176.2-99. Патент на схему истек только в 2008 году, но Шнорр лично разрешил ее использование в нашей стране.

А какие еще научные достижения у Клауса Шнорра? И сможете ли вы отличить их от достижений американского математика Питера Шора?

Ответ дать в виде строки длины 4 в алфавите {0, 1}. Пример: 0110.

0 (Шнорр) или 1 (Шор)	**0 или 1**	**0 или 1**	**0 или 1**
Квантовый алгоритм факторизации	Группа (алгебраическая)	Алгоритм построения короткого базиса решетки	Цикл стихов по мотивам книг Джорджа Мартина (Игра престолов)

30:00

Start

7 Она

Сначала у НЕЕ их было 3. Затем добавили еще 2, еще 2, еще 1 и стало можно выбирать 3 из 5, 7 и даже 8. А иногда можно быть добавить четвертый. В нашей стране ОНА появилась в 1995 году.

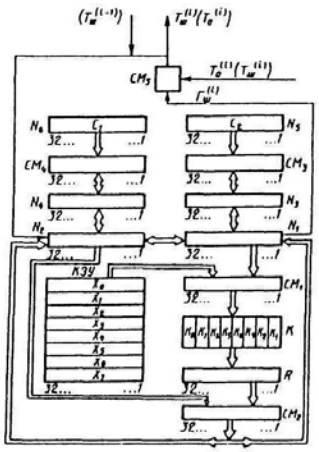
Кто такая ОНА?

Ответ дать одним словом.

30:00

Start

8 ГОСТ 28147



ГОСТ 28147 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования», принятый в 1989 году, стал советским ответом на коммерчески успешный американский DES (Data Encryption Standard). ГОСТ 28147 в первоначальном виде действует в нашей стране с 1992 года. В РФ базовый блочный шифр изменен, теперь он называется Магма. Принятие ГОСТ 28147 стало революционным шагом. Не только техническим, но и филологическим. В Приложении 1 были введены термины, до этого применяемые только в секретной государственной криптографии: гаммирование, гамма шифра, имитозащита, имитовставка, синхропосылка.

А как в этом приложении называются прямое и обратное преобразования?

A Зашифровывание и расшифровывание.

B Зашифрование и расшифрование.

C Зашифрование и расшифровка.

D Зашифровка и расшифровка.

30:00

Start

9 Фиалка, Самшит и другие

Фиалка (М-125) — советская шифровальная машина, разработанная вскоре после Второй мировой войны. Использовалась странами Варшавского договора вплоть до 1990-х годов.

А что советские военные криптографы кодировали словами Самшит, Кизил, Ячмень и Корвет?

A Преподавателей Факультета криптографии.

B Страны – потенциальные противники.

C Шифрмашины серии Фиалка.

D Кодировочные колеса (роторы) Фиалки.

30:00

Start

10 ЭЦП

В 1999 году был принят “Закон об электронном документе”. На тот момент подобного закона формально не было даже в США. Закон несколько раз обновлялся. Последние изменения сделаны в 2018 году.

А как в Законе 1999 года определяется ЭЦП?

A Набор символов, вырабатываемый средством электронной цифровой подписи при обработке электронного документа.

B Набор символов, вырабатываемый средствами электронной цифровой подписи и являющийся неотъемлемой частью электронного документа.

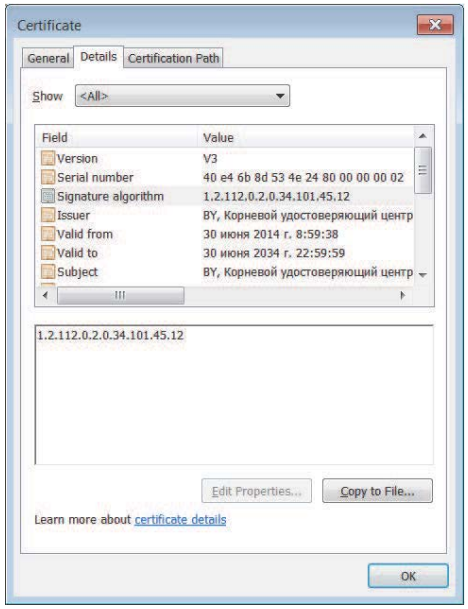
C Набор символов, вырабатываемый средствами электронной цифровой подписи и являющийся реквизитом электронного документа.

D Набор символов, являющийся реквизитом электронного документа и предназначенный для подтверждения его целостности и подлинности.

30:00

Start

11 ГосСУОК



ГосСУОК – Государственная система управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь – функционирует с 2014 года. Ее оператором является Национальный центр электронных услуг. На рисунке – сертификат Корневого удостоверяющего центра (КУЦ). От надежности защиты личного ключа КУЦ зависит безопасность всей инфраструктуры.

А сколько сертификатов выпущено в ГосСУОК к этому моменту?

A 250 тыс. – 500 млн.

B 500 тыс. – 1 млн.

C 1 млн. – 2 млн.

D 2 млн. – 4 млн.

30:00

Start

12 Холивар

При реализации алгоритмов СТБ 1176.2 возникли неожиданные технические трудности. Алгоритм выработки ЭЦП принимает на вход подписываемое сообщение M –

последовательность байтов, имеющая конечную длину

(определение СТБ). Но согласно распространенным программным криптографическим интерфейсам, которым безусловно требовалось следовать, алгоритм выработки ЭЦП принимает на вход не само сообщение M, а его хэш-значение h(M) –

последовательность байтов, имеющая фиксированную длину.

Некоторые посчитали, что можно разрешить передачу h(M) вместо M. Ведь хэш-значение сообщения также является сообщением (последовательностью байтов), причем h(M) однозначно характеризует M.

Другие были категорически против, настаивая на подписи исключительно M. Ведь h(M) не несет смысловой нагрузки, характерного для сообщений.

Споры затянулись на несколько лет. Вариант с подписью h(M) в конце концов был разрешен и даже стандартизирован. Но, все-таки, кто прав? Можно ли подписывать хэш?

А Да, ведь хэш является последовательностью байтов.

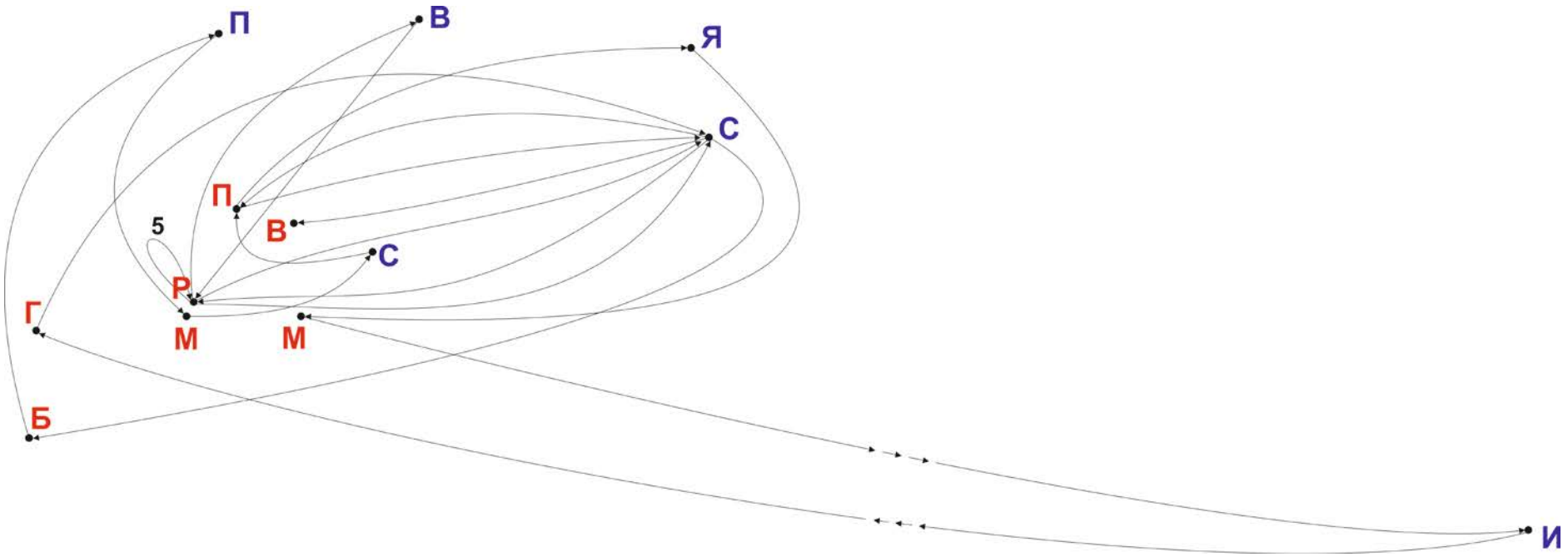
В Нет, ведь хэш не несет смысловой нагрузки.

30:00

Start

13 Криптограмма

Раскройте смысл следующей криптограммы:



Ответом должна быть аббревиатура из трех букв.

30:00

Start

14 Рускрипто 1999

Долгие годы Рускрипто была практически единственной конференцией по математической криптографии на постсоветском пространстве. На фотографии ниже – участники Рускрипто-1999. Мы скрыли 2 фигуры. Слева от фигуры № 1 (в первом ряду, очки, усы, без шапки) – Лебедев Анатолий Николаевич (ЛАН), главный организатор конференции. В 1991 году он основал компанию “ЛАН Крипто”, которая занималась созданием средств криптографической защиты информации. “ЛАН Крипто” участвовала в разработке СТБ 1176.2.

Чьи фигуры мы скрыли?

30:00

Start