Отчёт по Внешнему Курсу - Этап 3

Основы информационной безопасности

Чистов Д. М.

17 мая 2025

Российский университет дружбы народов, Москва, Россия

Объединённый институт ядерных исследований, Дубна, Россия

Цель работы _____

Цель работы

Пройти внешний курс - Этап 3

В лекционных материалах было сказано, что в протоколы прикладного уровня включён HTTPS

Выберите один вариант из списка Правильно, молодец!	Верно решили 940 учащихся Из всех попыток 42% верных
обе стороны имеют общий секретный ключ одна сторона публикует свой секретный ключ, другая - держит его в секрете одна сторона имеет только секретный ключ, а другая – пару из открытого и секретного ключей обе стороны имеют пару ключей Следующий шаг Решить снова	
<u>ш</u> 34 № 10 Шаг 3 Комментарии Решения	Следующий шаг 🗲

Рис. 1: Задание 001

Обе стороны имеют публичный ключ и секретный ключ, одна сторона открывает публичный ключ, а другая использует его для шифрования, но только владелец секретного ключа его расшифровывает

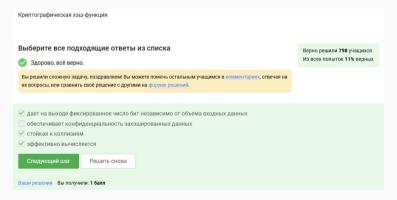


Рис. 2: Задание 002

Всё подходит, но очевидно, что хэш-функция не обеспечивает конфиденциальность

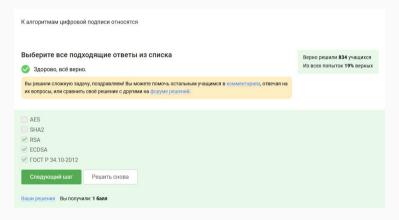


Рис. 3: Задание 003

Первые два ответа - никак не относятся к цифровой подписи, это алгоритм симметричного шифрования (AES) и хэш-функция



Рис. 4: Задание 004

Т.к. обе стороны по сути проверяются по одному ключу, следовательно это симметричная криптография

	Выберите один	вариант из списка		Верно решили 948 учащихся
асимметричный примитив генерации общего открытого ключа в асимметричный примитив генерации общего секретного ключа	Всё получило	ь!		Из всех попыток 47% верных
асимметричный примитив генерации общего открытого ключа ● асимметричный примитив генерации общего секретного ключа				
 асимметричный примитив генерации общего секретного ключа 	симметричный	примитив генерации об	цего секретного ключа	
	асимметричны	примитив генерации об	бщего открытого ключа	
	• асимметричны	примитив генерации об	бщего секретного ключа	
 асимметричный алгоритм шифрования 	асимметричны	алгоритм шифрования		
Следующий шаг Решить снова		Решить снова		

Рис. 5: Задание 005

Асимметричный, т.к. у каждой стороны и свой секретная и открытая часть, и он устанавливает ключ, но не шифрует

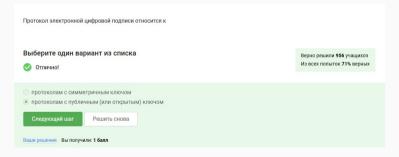


Рис. 6: Задание 006

Т.к. для подписей используется асимметричная криптография, следовательно это публичный протокол

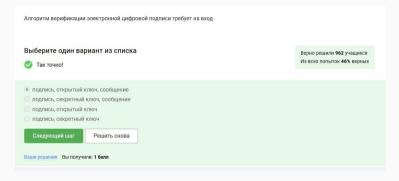


Рис. 7: Задание 007

Открытый ключ используется для расшифровки подписи, подпись это зашифрованный хэш, ну и сам хэш



Рис. 8: Задание 008

Конфиденциальность не обеспечивается, т.к. сообщение не шифруется

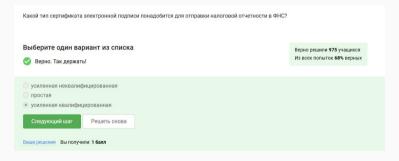


Рис. 9: Задание 009

Она создаётся с использование сертифицированных средств криптозащиты, а также имеет юридическую силу, что важно при работе с государством

Выберите один вариант из списка	Верно решил 971 учащийся Из всех попыток 61% верных
Правильно, молодец!	
в любой организации, имеющей соответствующую лицензию ФСБ	
в минкомсвязи РФ	
в удостоверяющем (сертификационном) центре	
в любой организации по месту работы	
Carrier Survey Daywood Province	
Следующий шаг Решить снова	

Рис. 10: Задание 010

Такие центры именно для этого и созданы, когда речь идёт о безопасности - это наилучший вариант, чем позволять выдавать сертификаты каждой желающей организации



13/21

SecurePay не считается, т.к. это электронная платёжная система, по сути и Bitcoin по этому не считается

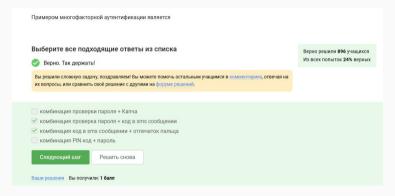


Рис. 12: Задание 012

Капча лишь может предотвратить (и то не всегда) автоматизированную атаку, а PIN-код + пароль тоже можно подобрать и не нужно иметь доступ к чему-нибудь стороннему (например, телефону)

Выберите один вариант	г из списка	Верно решили 957 учащихся Из всех попыток 59 % верных
многофакторная аутентиф	икация покупателя перед банком-эмитентом	
однофакторная аутентифи	кация покупателя перед банком-эквайером	
однофакторная аутентифи	кация при помощи PIN-кода карты перед терминалом	
S	икация покупателя перед банком-эквайером	

Рис. 13: Задание 013

Банк-эмитент - тот, кто выпустил карту, следовательно он несёт ответственность за аутентификацию пользователя, также используется многофакторная аутентификация - что-то, что знает пользователь + что-то, что этот пользователь имеет (телефон)

Какое свойство криптографической хэш-фун	кции используется в доказательстве работы?	
Выберите один вариант из списка		Верно решили 932 учащихся Из всех попыток 49 % верных
фиксированная длина выходных данных сложность нахождения прообраза обеспечение целостности эффективность вычисления Следующий шат Решить снова		

Рис. 14: Задание 014

При нахождении потребуется очень много вычислений, переборов - оттого и сложность, однако проверка результата будет быстрой

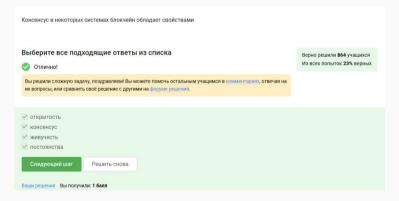


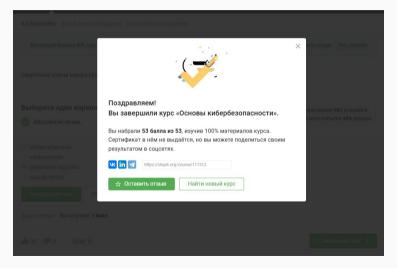
Рис. 15: Задание 015

Подходят все варианты

Секретные ключи какого кри	тографического примитива хранят участники блокч	ейна?
Выберите один вариан Абсолютно точно.	из списка	Верно решил 951 учащийся Из всех полыток 48 % верных
обмен ключамишифрованиецифровая подписьхэш-функция		
Следующий шаг Ре Ваши решения Вы получили: 1 6	лл	

Рис. 16: Задание 016

Курс успешно пройден



Выводы



Этап 3 пройден успешно на максимальный балл.

Список литературы

Список литературы

Курс "Основы Кибербезопасности" на платформе Stepik