Отчёт по выполнению стороннего курса

Информационная безопасность

Арбатова Варвара Петровна

Содержание

1	Выг	олнени	е зад	ани	1Й															6
	1.1	Этап 1																		6
	1.2	Этап 2																		22
	1.3	Этап 3															_			33

Список таблиц

Список иллюстраций

1.1	1						•					•					•					•		•			•	•	6
1.2	2	2			•	•	•		•			•		•															7
1.3	3	3										•																	8
1.4	4	ŀ	•									•										•					•		8
1.5	5	5										•				, ,													9
1.6	6	,																											9
1.7	7	7																											10
1.8	8	3																											11
1.9	9)																											12
1.10	1	.0																											12
1.11	. 1	1										•				, ,													13
1.12	1	2																											14
1.13	1	.3												•															15
1.14	1	4										•				, ,													16
1.15	1	5												•															17
1.16	1	6												•															18
1.17	1	7												•															18
1.18	3 1	8												•															19
1.19	1	9										•				, ,													20
1.20	2	20												•															21
1.21	2	21										•				, ,													21
1.22	2	2												•															22
1.23	1											•				, ,													23
1.24	2	2										•				, ,													24
1.25	3	3										•				, ,													25
1.26	4	ŀ					•							•															26
1.27	5	5										•				, ,													27
1.28	6	,										•				, ,													28
1.29	7	7										•				, ,													28
1.30	8	3										•				, ,													29
1.31	9)										•				, ,													29
1.32	1	0										•				, ,													30
1.33	1	1										•				, ,													30
1.34	1	2										•					•												31
1.35	5 1	.3										•					•												32
1.36	1	4										•																	32
1.37	, 1	5																											33

1.38 1	1	•	•	•	•	•	•		•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	33
1.39	2																	•																							•		34
1.40	3	•								•					•			•		•	•					•							•	•	•			•			•		34
1.41	4	•								•					•			•		•	•					•							•	•	•			•			•		35
1.42	5	•		•				•			•				•			•	•	•	•				•	•							•	•	•	•	•	•		•	•	•	36
1.43	6	•		•				•			•				•			•	•	•	•				•	•							•	•	•	•	•	•		•	•	•	36
1.44	7	•	•	•	•					•	•	•	•	•	•	•	•	•	•	•	•		•	•	•	•	•			•	•	•	•	•	•	•	•	•	•	•	•	•	37
1.45	8	•		•				•			•				•			•	•	•	•				•	•							•	•	•	•	•	•		•	•	•	38
1.46	9	•	•	•	•					•	•	•	•	•	•	•	•	•	•	•	•		•	•	•	•	•			•	•	•	•	•	•	•	•	•	•	•	•	•	38
1.47	10			•				•			•				•			•	•	•	•				•	•							•	•	•	•	•	•		•	•	•	39
1.48 3	11			•	•					•	•	•		•	•	•		•	•	•	•		•	•	•	•				•	•	•	•	•	•	•	•	•	•	•	•	•	39
1.49	12			•				•			•				•			•	•	•	•				•	•							•	•	•	•	•	•		•	•	•	40
1.50 3	13			•				•			•				•			•	•	•	•				•	•							•	•	•	•	•	•		•	•	•	40
1.51	14			•				•			•				•			•	•	•	•				•	•							•	•	•	•	•	•		•	•	•	41
1.52 3	15									•					•			•		•	•					•							•	•	•			•			•		41
1 52	16																																										42

1 Выполнение заданий

1.1 Этап 1

HTTPS - протокол прикладного уровня, выбираю его

Выберите протокол прикладного уровня

Выберите один вариант из списка

Всё правильно.

UDP TCP HTTPS											
Следующий шаг	Решить снова										
Ваши решения Вы получили: 1 балл											

Рис. 1.1: 1

ТСР работает на транспортном уровне

На каком уровне работает протокол ТСР?

Выберите один вариант из списка

Правильно, молодец!

Транопортном	
• Транспортном	
ПрикладномКанальном	
Сетевом	
Следующий шаг	Решить снова
Ваши решения Вы получи	или: 1 балл

Рис. 1.2: 2

Выбираю все корректные номера

Рис. 1.3: 3

DNS сервер сопоставляет IP адреса доменным именам

DNS сервер

Выберите один вариант из списка

🗸 Правильно.



Рис. 1.4: 4

Эта модель работает по такой последовательности, которую я выбрала

Выберите корректную последовательность протоколов в модели TCP/IP

Выберите один вариант из списка

Здорово, всё верно.

сетевой — прикладной — канальный — транспортный
прикладной — транспортный — канальный — сетевой
транспортный — сетевой — прикладной — канальный
прикладной — транспортный — сетевой — канальный
Решить снова

Рис. 1.5: 5

Этот протокол передает данные в открытом виде

Протокол http предполагает

Ваши решения Вы получили: 1 балл

Выберите один вариант из списка

Верно.

		у клиентом и сервером вером в открытом виде
Следующий шаг	Решить снова	
Ваши решения Вы получи	или: 1 балл	

Рис. 1.6: 6

Так как данные в открытом виде, шифрование не нужно, задачи этого протокола не включают аутентификацию

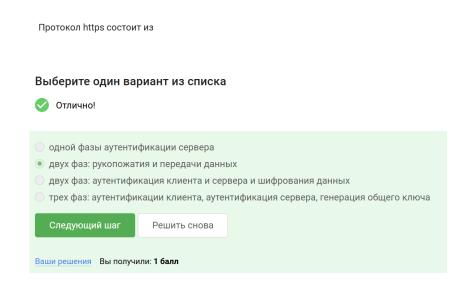


Рис. 1.7: 7

Это происходит с обеих сторон

Выберите один вариант из списка

🗸 Здорово, всё верно.

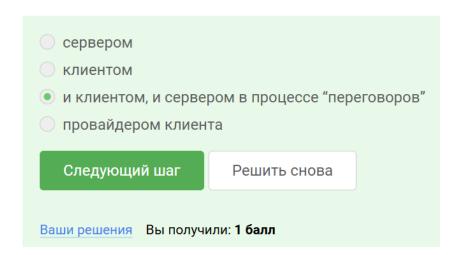


Рис. 1.8: 8

Этот протокол в фазе рукопожатия не предусматривает шифрование данных

В фазе "рукопожатия" протокола TLS не предусмотрено

Выберите один вариант из списка Хорошая работа. формирование общего секретного ключа между клиентом и сервером аутентификация (как минимум одной из сторон) выбираются алгоритмы шифрования/аутентификации шифрование данных Следующий шаг Решить снова Ваши решения Вы получили: 1 балл

Рис. 1.9: 9

Выбираю, что хранят куки

Куки хранят:	
Выберите все подх	одящие ответы из списка
🗸 Верно.	
	чу, поздравляем! Вы можете помочь остальным учащимся в комментариях, пи сравнить своё решение с другими на ф <u>оруме решений</u> .
 идентификатор поль 	зователя
ІР адрес	
✓ id сессии	
пароль пользовател	4
Следующий шаг	Решить снова
Ваши решения Вы получи	ли: 1 балл

Рис. 1.10: 10

Куки никак не связаны с улучшением надежности соединения

Выберите один вариант из списка

\bigcirc	Хорошая работа.

аутентификации пол	IL SOPSTORE											
персонализации веб	5-страниц											
отслеживания инфо	рмации о пользователе											
Сборе статистики по	сещаемости сайта											
• улучшения надежно	сти соединения											
Следующий шаг	Решить снова											
Ваши решения Вы получили: 1 балл												

Рис. 1.11: 11

Клиент не занимается генерацией куки, это делает сервер

Куки генерируются

Выберите один вариант из списка

Правильно, молодец!

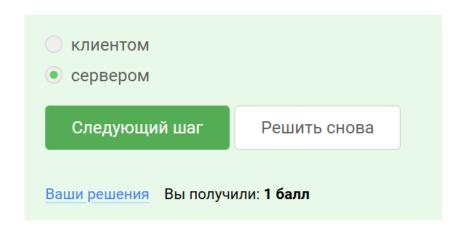


Рис. 1.12: 12

Выбираю правильный ответ

Сессионные куки хранятся в браузере?

Выберите один вариант из списка

Верно. Так держать!

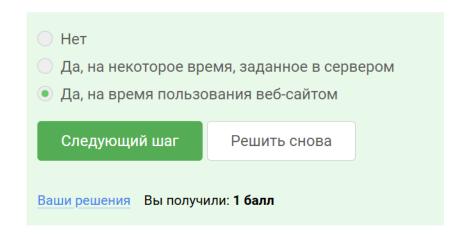


Рис. 1.13: 13

В этой луковой сети 3 промежуточных узла

Сколько промежуточных узлов в луковой сети TOR?

Выберите один вариант из списка

Дабсолютно точно.
 2
 3
 4
 Следующий шаг
 Решить снова

Ваши решения
Вы получили: 1 балл

Рис. 1.14: 14

ІР-адрес получателя известен отправителю и выходному узлу

Ваши решения Вы получили: 1 балл

Выберите все подходящие ответы из списка ✓ Здорово, всё верно. Вы решили сложную задачу, поздравляем! Вы можете помочь остальн отвечая на их вопросы, или сравнить своё решение с другими на фору! □ охранному узлу □ промежуточному узлу ✓ отправителю ✓ выходному узлу Следующий шаг Решить снова

Рис. 1.15: 15

Выбираю правильный ответ

Выберите один вариант из списка

Всё получилось!
 только с охранным узлом
 с охранным и промежуточным узлом
 с охранным, промежуточным и выходном узлом
 с промежуточным и выходным узлом
 Следующий шаг
 Решить снова

Ваши решения
Вы получили: 1 балл

Рис. 1.16: 16

Для этого подходит любой браузер, поэтому нет

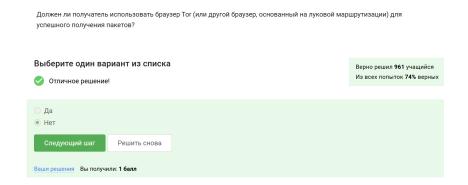


Рис. 1.17: 17

Это определение Wi-Fi

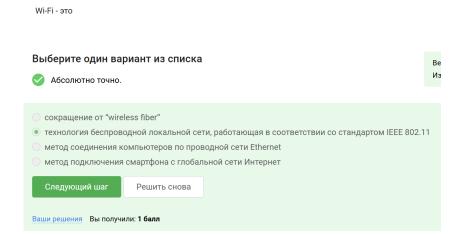


Рис. 1.18: 18

Это тоже факт

На каком уровне работает протокол WiFi?

Выберите один вариант из списка

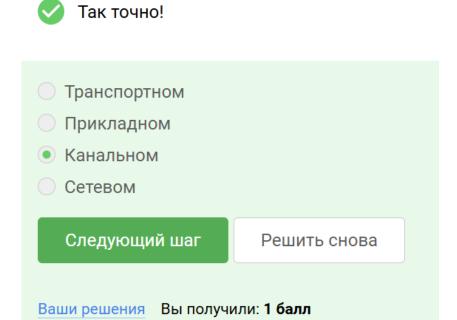


Рис. 1.19: 19

Выбираю небезопасный метод

Рис. 1.20: 20

Это делается для безопасности

Данные между хостом сети (компьютером или смартфоном) и роутером

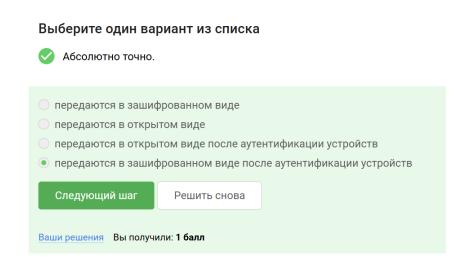


Рис. 1.21: 21

Выбирают метод

Для домашней сети для аутентификации обычно используется метод

Рис. 1.22: 22

1.2 Этап 2

Это правда

Можно ли зашифровать загрузочный сектор диска

Выберите один вариант из списка

Хорошие новости, верно!

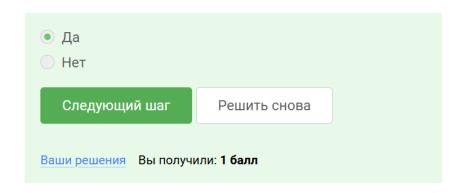


Рис. 1.23: 1

Шифрование диска основано на симметричном шифровании

Шифрование диска основано на

Выберите один вариант из списка

🗸 Всё правильно.

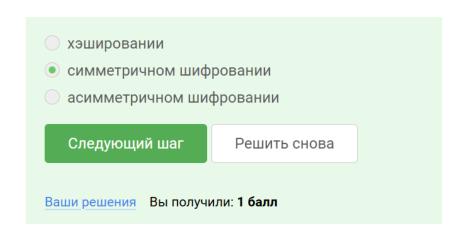


Рис. 1.24: 2

Выбираю программы для зашифровки жесткого диска

С помощью каких программ можно зашифровать жесткий диск?

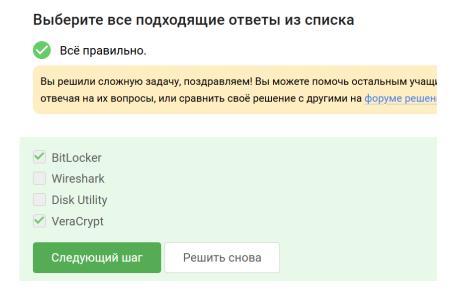


Рис. 1.25: 3

Этот пароль можно отнести к стойким, так как он содержит и строчные, и заглавные буквы, цифры, специальные знаки

Какие пароли можно отнести с стойким?

Выберите один вариант из списка

🗸 Всё правильно.

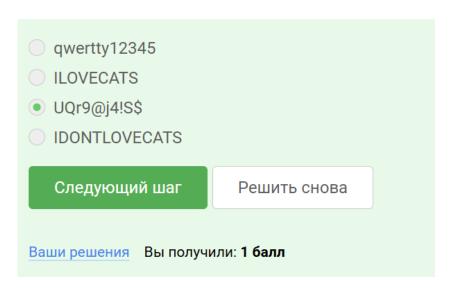


Рис. 1.26: 4

Менеджер паролей специально предназначен для безопасного хранения паролей

Где безопасно хранить пароли?

Выберите один вариант из списка

🗸 Верно. Так держать!

© B											
В менеджерах паро.	леи										
В заметках на рабоч	нем столе										
🔘 В заметках в телефо	оне										
На стикере, приклее	енном к монитору										
🔾 В кошельке											
Следующий шаг	Решить снова										
Ваши решения Вы получили: 1 балл											
	······										

Рис. 1.27: 5

Выбираю предназначение капчи

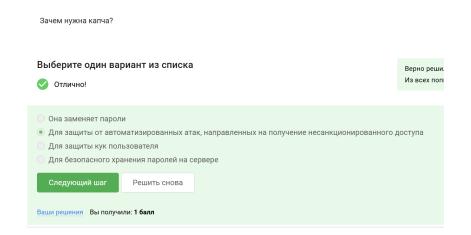


Рис. 1.28: 6

Хэширование нужно, чтобы не хранить пароли на сервере в открытом виде

Для чего применяется хэширование паролей?

Выберите один вариант из списка

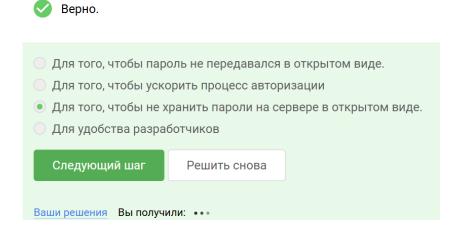


Рис. 1.29: 7

Это правда

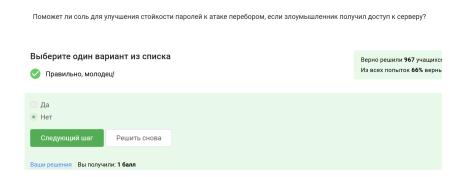


Рис. 1.30: 8

Выбираю все, так как все представленные меры защищают от утечек данных атакой перебором

Какие меры защищают от утечек данных атакой перебором?

Выберите все подходящие ответы из списка Так точно! Вы решили сложную задачу, поздравляем! Вы можете помочь остальным отвечая на их вопросы, или сравнить своё решение с другими на форуме розные пароли на всех сайтах териодическая смена паролей сложные(=длинные) пароли капча Следующий шаг Решить снова Ваши решения Вы получили: 1 балл

Рис. 1.31: 9

Смотрю ссылки реальные и сравниваю с представленными

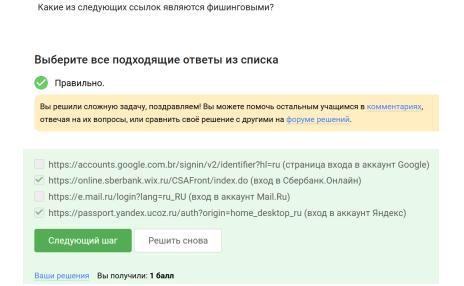


Рис. 1.32: 10

Может. Человека могли взломать, он мог ошибиться

Выберите один вариант из списка

Может ли фишинговый имейл прийти от знакомого адреса?

Правильно. Да Нет Следующий шаг Решить снова Ваши решения Вы получили: 1 балл

Рис. 1.33: 11

Это определение

Выберите один вариант из списка

Здорово, всё верно.

протокол для отпра	вки имейлов										
метод предотвраще	ения фишинга										
🔾 атака перебором па	ролей										
• подмена адреса отп	правителя в имейлах										
Следующий шаг	Решить снова										
Ваши решения Вы получили: 1 балл											

Рис. 1.34: 12

Это определение

Вирус-троян

Выберите один вариант из списка

Ваши решения Вы получили: 1 балл

✓ Верно. Так держать!
 ○ обязательно шифрует данные и вымогает ключ дешифрования
 ○ маскируется под легитимную программу
 ○ работает исключительно под ОС Windows
 ○ разработан греками
 Следующий шаг
 Решить снова

Рис. 1.35: 13

Это факт

На каком этапе формируется ключ шифрования в протоколе мессенджеров Signal?

Выберите один вариант из списка

✓ Прекрасный ответ.

при генерации первого сообщения стороной-отправителем
при установке приложения
при каждом новом сообщении от стороны-отправителя
при получении сообщения

Следующий шаг
Решить снова

Рис. 1.36: 14

Выбираю суть сквозного шифрования

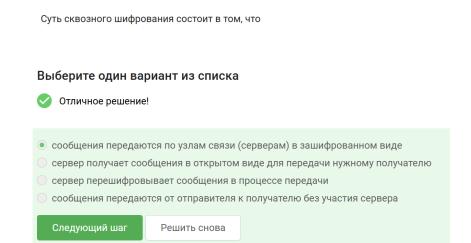


Рис. 1.37: 15

1.3 Этап 3

Это факт

В асимметричных криптографических примитивах	
Выберите один вариант из списка Всё правильно.	
одна сторона имеет только секретный ключ, а другая — пару из открытого и секретнобе стороны имеют общий секретный ключ одна сторона публикует свой секретный ключ, другая - держит его в секрете обе стороны имеют пару ключей	ого ключей
Следующий шаг	
Ваши решения Вы получили: 1 балл	

Рис. 1.38: 1

Из всего эта хэш-функция только не обеспечивает конфиденциальность захэшированных данных

Криптографическая хэш-функция

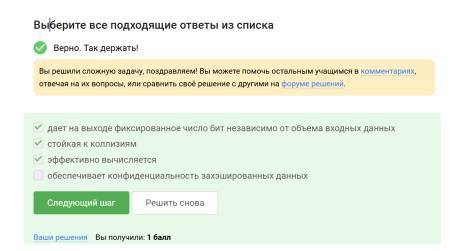


Рис. 1.39: 2

Первые 2 не относятся

К алгоритмам цифровой подписи относятся

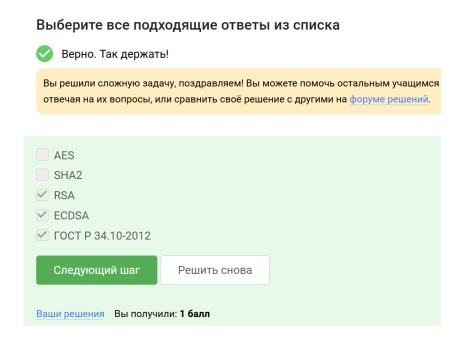


Рис. 1.40: 3

Это факт

Код аутентификации сообщения относится к

Выберите один вариант из списка

🗸 Здорово, всё верно.



Рис. 1.41: 4

Это определение

Выберите один вариант из списка ✓ Так точно! Симметричный примитив генерации общего секретного ключа асимметричный примитив генерации общего открытого ключа асимметричный примитив генерации общего секретного ключа асимметричный алгоритм шифрования Следующий шаг Решить снова Ваши решения Вы получили: 1 балл

Рис. 1.42: 5

Это факт

Протокол электронной цифровой подписи относится к

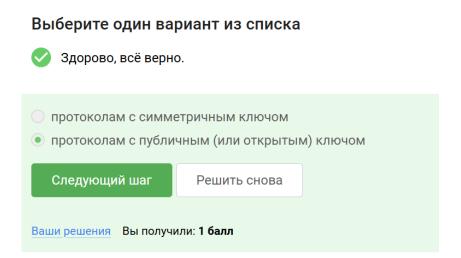


Рис. 1.43: 6

Это было сказано в видео

Алгоритм верификации электронной цифровой подписи требует на вход

Выберите один вариант из списка Отличное решение! подпись, секретный ключ подпись, открытый ключ подпись, секретный ключ, сообщение подпись, открытый ключ, сообщение Следующий шаг Решить снова Ваши решения Вы получили: 1 балл

Рис. 1.44: 7

Правда, ключ открытый, например

Выберите один вариант из списка

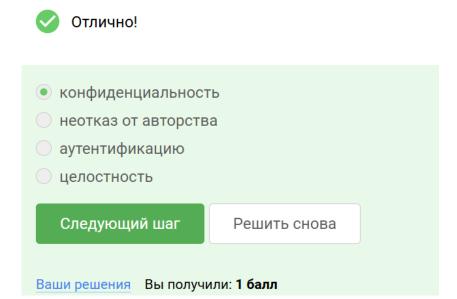


Рис. 1.45: 8

Это требование

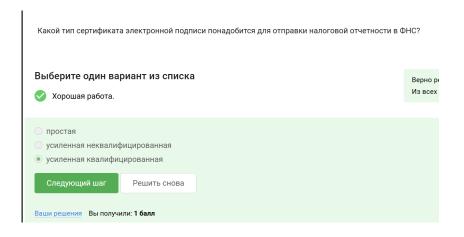


Рис. 1.46: 9

Это специализированный центр

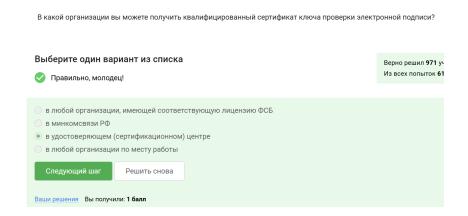


Рис. 1.47: 10

Все остальное - криптовалюта, методы снятия или пополнения денег со счёта и так далее

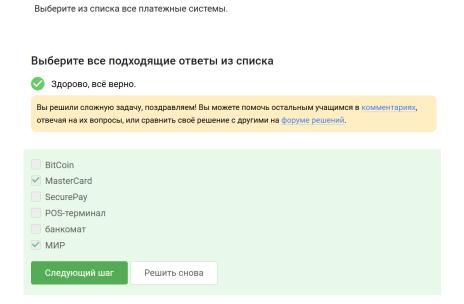


Рис. 1.48: 11

Все остальное не является

Выберите все подходящие ответы из списка ✓ Хорошие новости, верно! Вы решили сложную задачу, поздравляем! Вы можете помочь остальным учаш отвечая на их вопросы, или сравнить своё решение с другими на форуме реше комбинация проверки пароля + Капча ✓ комбинация проверка пароля + код в sms сообщении ✓ комбинация код в sms сообщении + отпечаток пальца комбинация РІN код + пароль Следующий шаг Решить снова

Рис. 1.49: 12

Для защиты используется то, что я выбрала

Ваши решения Вы получили: 1 балл

Рис. 1.50: 13

Это факт

Какое свойство криптографической хэш-функции используется в доказательстве работы?

Выберите один вариант из списка

Хорошие новости, верно!

фиксированная длина выходных данных

сложность нахождения прообраза

обеспечение целостности

эффективность вычисления

Следующий шаг

Решить снова

Рис. 1.51: 14

Всё выбранные свойства нам подходят

Консенсус в некоторых системах блокчейн обладает свойствами

Выберите все подходящие ответы из списка ✓ Так точно! Вы решили сложную задачу, поздравляем! Вы можете помочь остальным учаготвечая на их вопросы, или сравнить своё решение с другими на форуме реше ✓ постоянства ✓ консенсус ✓ открытость ✓ живучесть Следующий шаг Решить снова Ваши решения Вы получили: 1 балл

Рис. 1.52: 15

Цифровая подпись, которой и был посвящен этот раздел

Секретные ключи какого криптографического примитива хранят участники блокчейна?

Выберите один вариант из списка

Обмен ключами

Шифрование

Цифровая подпись

хэш-функция

Следующий шаг

Решить снова

Ваши решения Вы получили: 1 балл

Рис. 1.53: 16