Iniciado em	quinta, 20 Jun 2024, 23:08
Estado	Finalizada
Concluída em	quinta, 20 Jun 2024, 23:12
Tempo empregado	3 minutos 1 segundo

Questão 1

Correto

Vale 1,00 ponto(s).

Elliptic Curve Diffie-Hellman é um método para troca de chaves que usa curvas eliptícas e aritmética modular de forma que Alice e Bob consigam a mesma chave.

Considere os valores abaixo:

E1: $y^2 = x^3 + 2.x + 2$

Um ponto G =

(366188872044353481590011866269107634 20,

111276197457777389520411166799612307 02)

in E1

p = 629483655670773810767857494374662893 89

Número de pontos em E1 = 629483655670773810901975542155940299 96

Alice gera um valor aleatório a = 123456789012345678901234567 89, gera o ponto A e envia para o Bob.

Bob envia o ponto B =

(192837398809241149965317972161995303 58,
409557822769835342619244767606452125 00) para Alice.

Agora Alice e Bob conseguem calcular um valor V comum aos dois.

Você não precisa saber o valor b que Bob gerou aleatoriamente, nem o valor A que a Alice calculou para achar o ponto V.

Assim, qual o Ponto V calculado para a geração da chave comum entre Alice e Bob? Colocar (x,y) sem espaços.

Resposta: (362117078153380949402062589536728634 83,422565668951207 ✔

Questão 2

Correto

Vale 1,00 ponto(s).

Dado o ponto V da questão anterior.

Sabe-se que para gerar a chave k, Alice e Bob usam SHA256 e pegam os primeiros 128 bits do resultado.

Ou seja, para, por exemplo, o ponto V = (11223344,55667788), usar o comando (no Linux) "echo 1122334455667788 | shasum -a 256" e pegar os 128 primeiros bits do resultado.

Assim, qual a chave k utilizada para troca de mensagens? (em hexa)

Resposta: 54e2df13054c85b7f7c7308def8bef8b ✔

Questão 3

Correto

Vale 1,00 ponto(s).

Dado a chave k da questão anterior, Alice manda a seguinte mensagem cifrada usando AES com CTR mode

c = AES(k, m) com modo CTR =

D59D64D83AA6C17BAD5B7386978962B6B21AA267354BE5AA29C4

IV utilizado = 01010101010101010101010101010101

O que a mensagem diz?

Resposta: Muito bem. Atingiu o topo. ✔