Faculdade SENAC de Porto Alegre
Segurança em Sistemas – 2017/II
Prof. Filipo Mór
www.filipomor.com
Revisão Geral

Criptografia

Assinale quais das seguintes afirmações são verdadeiras.

( ) a técnica criptográfica RSA depende do uso de dois números compostos para a geração do par chave pública e chave privada.
( ) chaves RSA de 768 bits são consideradas seguras atualmente.
( ) a técnica de criptografia ElGamal apresenta um custo computacional maior do que a técnica RSA.
( ) a técnica SHA-256 é utilizada para a geração de chaves públicas e chaves privadas.
( ) considerando o uso da técnica RSA como assinatura digital, a chave privada deve ser mantida sigilosa para que a segurança seja garantida.
( ) uma chave publica RSA gerada a partir dos números primos 11 e 13 possui 12 bits de comprimento.
( ) a técnica SHA-256 não pode ser associada a técnica RSA.
( ) a técnica RSA pode ser associada a uma técnica de cifras para a definição do alfabeto de símbolos.

Considerando o funcionamento da blockchain do Bitcoin, conforme estudado em aula, responda as seguintes questões:

1. Como uma transação adicionada a um bloco é validada pelo sistema?
2. O que ocorreria se um bloco fraudulento fosse submetido a uma nodo em específico da blockchain, de forma que o usuário malicioso pudesse efetuar um "gasto duplo" utilizando os mesmos créditos?
3. Como funciona o incremento na dificuldade de mineração que ocorre no bitcoin de tempos em tempos?
4. Quando a quantidade máxima de bitcoins tiver sido finalmente minerada (21 milhões de bitcoins), que dispositivo servirá de incentivo aos mineradores? E como este dispositivo funciona?
5. O que impacta mais o tempo de transação do bitcoin? A latencia de rede, a obtenção do consenso ou a quantidade de transações existentes no ether no momento? Justifique sua resposta.
6. Quais são os principais problemas da blockchain do bitcoin que impedem a sua adoção em massa como forma de pagamento e consumo?
7. Qual é a justificativa para que a rede VISA tenha uma capacidade tão maior de transações do que a blockchain do bitcoin?
8. Que dispositivo serve de incentivo para os nodos da blockchain Etherium executarem smart contracts?
9. Como funciona a técnica da Prova de Trabalho (*Proof of Work*)?
10. De onde advém o valor atribuído ao bitcoin, considerando que consiste em um moeda "sem lastro"?