Lista de exercícios: MAC

1. O que é e para que serve um Message Authentication Code?

2. Quais são os serviços de segurança que podem ser alcançados com um MAC?

3. Qual é a relação entre um MAC e uma função hash?

4. Qual é a relação entre um MAC e uma cifra de blocos?

5. Explique como funciona o CBC-MAC.

6. Relacione um MAC com uma assinatura digital.

7. Para funções hash é crucial ter um grande número de bits de saída, por exemplo 160 bits, para proteção contra "ataques do paradoxo do aniversário". Porque para MAC apenas 80 bits são necessários?

8. Mostre que a construção básica CBC-MAC não é segura quando considerando mensagens de tamanhos diferentes.

9. Prove que a construção básica CBC-MAC não é segura se um IV aleatório. Comente um caso de mundo-real onde o ataque de um IV aleatório pode ser usado.

10. O que é integridade?

11. Explique como funciona encriptação autenticada e contra qual tipo de atacante ela é eficaz.

12. O que é HMAC?