Lista de exercícios: Assinaturas

1. Porque assinaturas digitais são importantes?

2. Quais são as características de segurança que assinaturas digitais provêm?

3. Qual é a diferença entre MAC e assinatura digital?

4. Explique como funciona o ECDSA.

5. Explique como funcionam assinaturas com RSA sem padding.

6. Explique como funcionam 3 ataques contra assinaturas com RSA sem padding.

7. Considerando assinatura com RSA usando chave públic ($n = 9797, e = 131$) quais assinaturas a seguir são seguras?

- $(x = 123, sign(x) = 6292)$
- $(x = 4333, sign(x) = 4768)$
- $(x = 4333, sign(x) = 1424)$

8. Um pintor tem uma nova ideia de modelo de negócios. Ele quer oferecer um serviço de pintura de quadros sob demanda. Os clientes poderão enviar fotos que serão transformadas em quadros. As fotos e as pinturas digitalizadas serão transmitidas de forma digital pela Internet. Uma preocupação dele é a privacidade dos clientes que podem querer enviar fotos que não podem ser vistas por terceiros. Portanto, a transmissão das imagens deve ser segura. O pintor necessita de várias semanas para a criação de uma obra e, portanto, quer ter certeza que não será enganado por alguém que envia uma foto sob um nome falso. Ele também quer ter certeza que a obra não poderá ser recusada pelo cliente, uma vez encomendada.

Descreva uma maneira de viabilizar esse modelo de negócios com enfoque nos requisitos de segurança de informação. Quais elementos criptográficos podem ser usados para cada requisito de segurança? Assuma que muitos megabytes são transmitidos para cada foto.

9. Dado um esquema de assinaturas RSA com chave pública ($n = 9797, e = 131$), descreva como um atacante pode realizar um ataque de falsificação de assinatura. Dê um exemplo desse ataque para esses parâmetros.

10. Em um esquema de assinatura digital RSA, Bobo assina mensagens x_i as envia juntas com as correspondentes assinaturas s_i e a chave pública para Alice. A chave pública de Bob é o par (n, e) e chave privada é d.

Um atacante pode executar o ataque de man-in-the-middle. O objetivo do atacante é alterar as mensagens e as assinaturas digitais que serão verificadas corretamente por Alice. Mostre as operações que o atacante deve fazer para um ataque ser bem sucedido.