Lista de exercícios: Troca de chaves Diffie-Hellman, Logaritmo discreto e El Gamal

1. Descreva passo a passo como funciona a troca de chaves de Diffie-Hellman. Porque ela é considerada segura?

2. O que são os problemas de logaritmo discreto?

3. Quais são as diferenças entre o problema computacional de logaritmo discreto e o problema decisional?

4. Descreva passo a passo como funciona o esquema de encriptação El Gamal.

5. Porque é necessário usar chaves efêmera no esquema de encriptação El Gamal?

6. Considere a encriptação El Gamal usando o grupo $\mathbf{Z}_{19}^*$

- Mostre que esse grupo é cíclico.
- Quantos elementos estão no grupo.
- Encontre um elemento no grupo que não é gerador (com exceção do elemento neutro)
- Assuma que alguém recebe um número primitivo desse grupo e escolhe expoente privado igual a 7. Qual deve ser a chave pública?
- Usando a chave pública do item anterior, qual seria a encriptação de $m = 2$?

7. Descreva os seguintes ataques contra problemas de logaritmo discreto

- Força bruta
- Método passo de bebê, passo de gigante
- Método Rho de Pollard
- Método de Pohlig-Hellman
- Método Index-Calculus

8. O que é o Teorema do Resto Chinês e qual é a sua relação com o ataque de Pohlih-Hellman e o sistema RSA?