MAC0336/5723 - Criptografia e Segurança de Dados - Lista de exercícios 3 (USP 2019)

- prazo de entrega: veja na página paca.ime.usp.br
- resolver *individualmente*, duas soluções idênticas receberão nota zero na lista toda
- entregue as suas soluções na página paca.ime.usp.br, em formato PDF
- MANUSCRITOS terão nota zero
- escreva no cabeçalho o seu NUSP e nome completo

Exercício 1 (25%) Para o Jogo de Cara-Coroa (Blum, pg 182), pergunta-se:

1. Em qual situação Beto ganha o jogo? Justifique a sua resposta. Nesse caso, por quê Alice aceita que Beto ganhou o jogo?
2. Em qual situação Alice ganha o jogo? Justifique a sua resposta. Nesse caso, por quê Beto aceita que Alice ganhou o jogo?
3. Justifique porque Beto rejeita o caso $y = 0$
4. Para $p = 3, q = 7, x = 4$, calcular $a, y, mdc(x + y, n)$

Exercício 2 (25%) Para o Protocolo de identificação FFS (pg 183) pede-se:

1. Demonstrar algebricamente que se y for autêntico, então de fato $y^2 = xv^e \bmod n$ ocorre.
2. Quais são os parâmetros de segurança e quais são os respectivos problemas computacionais que protegem esses parâmetros? Por quê o conhecimento desses parâmetros gera insegurança?
3. Por quê esse protocolo é do tipo Zero Knowledge?
4. Para os dois casos: $e = 1, e = 0$, dados $t = 1, p = 3, q = 7, s = 17, r = 13$, calcular $v, x, y = rs^e \bmod n$, $y^2 \bmod n$, $xv^e \bmod n$ e verificar que, de fato, $y^2 = xv^e \bmod n$

Exercício 3 (25%) No protocolo de identificação GQ (pg. 186), pede-se:

1. Demonstrar algebricamente que se s_A for autêntico, então de fato $z = x \bmod n$ ocorre.
2. Justificar porque o caso $z = 0$ deve ser rejeitado
3. Verificar ou justificar que $mdc(v, \Phi(n)) = 1, mdc(J_A, \Phi(n)) = 1$
4. Por quê essas condições $mdc(v, \Phi(n)) = 1, mdc(J_A, \Phi(n)) = 1$ são exigidas?
5. Quais são os parâmetros de segurança e quais são os respectivos problemas computacionais que protegem esses parâmetros? Por quê o conhecimento desses parâmetros gera insegurança?
6. Por quê esse protocolo é do tipo Zero Knowledge?
7. Para $p = 7, q = 13, v = 11, J_A = 29, r = 13, e = 6$, calcular: $n, \Phi(n), s, s_A, x, y, z$ e verificar que, de fato, $z = x$.

Exercício 4 (25%) No algoritmo de assinatura Schnorr (pg. 209 do livro), supor, para α, β decimais, que $h(\alpha) = \alpha^3 \bmod 13$, e $\alpha || \beta$ significa dígitos de α seguidos pelos dígitos de β; por exemplo $72||09 = 7209$. Se g é um gerador $\bmod p$, $b = g^{(p-1)/q} \bmod p$

Pede–se:

1. Demonstrar algebricamente que a assinatura é válida se e só se $e = e'$
2. O algoritmo de assinatura Schnorr é mais rápido do que o algoritmo de verificação? Justifique a sua resposta.
3. Como uma falsa Alice, sem conhecer o segredo S da Alice, poderia falsificar uma assinatura Schnorr sobre um texto x?
4. Qual é a probabilidade de sucesso de tal falsificação? Justifique a sua resposta. Sugestão: aplicar o Paradoxo do Aniversário (pg. 219).
5. Quais são os parâmetros de segurança e quais são os respectivos problemas computacionais que protegem esses parâmetros? Por quê o conhecimento desses parâmetros gera insegurança?
6. Para os valores $p = 17, q = 8, g = 7, x = 12, s = 9, r = 6$ calcular b, v, u, e a assinatura Schnorr (y, e) sobre x.
7. Calcular $z = b^y v^e \bmod p$, e $e' = h(x||z)$. E verificar que, de fato, $e = e'$

FIM FIM FIM FIM FIM