

# Criptografia 2020

Matheus T. de Laurentis, 9793714

Q1.

1) O tamanho, em bits, vale:

$$\bullet X: \lceil \log_2 p \rceil$$

$$\bullet e: t$$

$$\bullet y: \lceil \log_2 q \rceil$$

$$\bullet z: \lceil \log_2 p \rceil$$

2)

Mesmo com coleção de mensagens verdadeiras trocadas, uma pessoa mal-intencionada poderá, apenas, personificar Alice com uma chance muito baixa.  $\frac{1}{2^t}$ .

O problema do logaritmo discreto protege o valor de  $r$ , pois, mesmo sabendo  $x, b, p$ , um invasor não conseguirá encontrar  $r$  pela expressão  $x = b^r \mod p$ . Por não conseguir  $r$ , ele também não poderá obter  $s$  através da expressão  $y = (se + r) \mod q$ . Porém, o invasor pode mesmo que saiba  $y, e$  e  $q$ .

3. Identificação Zero Knowledge é um método de um indivíduo mostrar aos demais que ele possui certa informação sem fornecê-la e sem qualquer outra informação adicional, com uma probabilidade arbitrariamente grande. O protocolo descrito é Zero Knowledge, pois, a única informação que Alice tem, e Beto não, é o valor de  $s$ . Além disso,

em nenhum dos passos ela utiliza de outras informações para responder Beto e, no fim dos passos, Beto sabe, com grande probabilidade, que Alice conhece o valor de  $S$ .

~~4. Como de resto, todas as pessoas, por exemplo, Beto, recebem diretamente de T os valores  $p, q, b$ .~~

4. Beto pode ~~sempre~~ solicitar que T assine  $(I_A, v)$  de Alice e comparar com o valor do certificado da chave pública.

6. Temos:

$$z = b^y v^e \bmod p$$

$$z = b^{se} \cdot b^r \cdot v^e \bmod p$$

$$z = (b^s \cdot v)^e \cdot b^r \bmod p$$

$$z = (b^s \cdot b^{-s})^e \cdot b^r \bmod p$$

$$z = b^r \bmod p = X$$

7. Como visto em (2), Carlos não pode descobrir os parâmetros privados de Alice. Ele pode, porém, chutar um valor de  $e$  no passo (1) e, com um  $y$  qualquer, enviar  $x = b^y v^e \bmod p$  no passo 1 e invocar  $y$  no passo 3. Contudo, a probabilidade de acertar o valor de  $e$  é  $1/2^t$ .



8. O ataque 'known plaintext attack' se tornaria possível. Poderiamos duas escolhas no valor de  $e$  para se conseguir o valor de  $S$ , pois, como resposta ao passo 3, respondendo  $e_2 = e_1 + 1$ :

$$y_1 = (S e_1 + r) \bmod p$$

$$y_2 = (S e_2 + r) \bmod p$$

$$y_1 - y_2 = S e_1 - S e_2 \bmod p = S$$

Com o valor de  $S$ , a personificação também se torna possível.

9. Se  $e$  e  $e'$  é constante a personificação é possível. Como descrito em (7) basta-se um mal-intencionado escolher  $y$  qualquer e enviar  $b^y v^e$  no passo 1 e  $y$  no passo 3 para enganar o Beto.

10. Alice pode calcular o testemunho  $x$  e Beto o desafio  $e$  antes do protocolo ser executado, porém, é improvável que a ordem das trocas de informações seja mantida



Q2

1. O autor da assinatura, que conhece o valor de  $s$ , é necessário para a assinatura. Isso ocorre, pois o cálculo de  $A$  requer o valor de  $sR$ , que não poderia ser enviado a um terceiro, pois este também precisaria do valor de  $R$  para assinar e, com  $sR$  e  $R$ , ele poderia descobrir  $s$ , por saber  $P$  e  $sP$  também.
2. A verificação não exige o autor, pois, o valor de  $s$  não é necessário em nenhuma de suas etapas.
3. Mesmo com uma coleção de assinaturas e mensagens ele não conseguiria falsificar a assinatura. Isso ocorre, pois, o problema do logaritmo discreto protege o valor de  $K$ , apesar de Carlos conhecer  $(x_1, y_1) = P$  no passo 1. Sem saber  $K$ , ele não pode descobrir  $s$  no passo 2.

5. Sabemos  $1 \leq R \leq p-1$ ,  $1 \leq A \leq p-1$

$$\begin{aligned}(x_0, y_0) &= v_1 P + v_2 Q \\&= H(m) A^{-1} P + R A^{-1} Q \\&= A^{-1} (H(m) P + R Q) \\&= A^{-1} (H(m) P + R s P) \\&= A^{-1} (H(m) + R s) P \\&= h_2 (H(m) + R s)^{-1} (H(m) + R s) P \\&= h_2 P\end{aligned}$$

$$V = x_0 = x_1 = R.$$

9. ~~Uma~~ Uma forma de tentar obter o  $S$  é:

~~Encontra  $V_1, V_2, P$~~

10. A verificação é mais custosa que a assinatura, pois a operação mais custosa é a multiplicação de escalar por coordenadas na curva, e, a verificação faz mais operações desse tipo