Criptografia 2020

Matheus T. de Laurentys, 9793714

Q1.

1) Os tamanhos, em bits, valem:
   - $x: \lceil \log_2 p \rceil$
   - $e: t$
   - $y: \lceil \log_2 q \rceil$
   - $z: \lceil \log_2 p \rceil$

2) Mesmo com coleção de mensagens verdadeiras trocadas, uma pessoa mal-intencionada poderá, apenas, personificar Alice com uma chance muito baixa. ~~$1/q^t$~~.

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

3. Identificação Zero Knowledge é ~~um método~~ um método de um indivíduo mostrar aos demais que ele possue 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 saberá, com grande probabilidade, que Alice conhece o valor de S.

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

5 Beto pode solicitar que T assine (I_A, V) de Alice e comparar com o valor do certificado da (chave pública) da 1ª etapa do protocolo de identificação.

6. Temos:

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

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

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

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

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

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 enviar y no passo 3. Concluo, a probabilidade de acertar o valor de e é $1/2^t$.

4. Após concluir a comunicação com Alice, se $z = x$, então b, p, q de Alice são os certos, pois, Beto usa o b e o p de T em seus cálculos e o resultado foi o mesmo do informado por Alice na 1ª etapa: $x = b_{ALICE}^{r} \bmod p_{ALICE}$

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

$$y_1 = (Se_1 + r) \bmod p$$
$$y_2 = (Se_2 + r) \bmod p$$
$$y_1 - y_2 = Se_1 - Se_2 \bmod p = S$$

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

9. Se o e é constante a personifição 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 imprescindível que a ordem das trocas de informação 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) e P no passo 1. Sem saber K, ele não pode descobrir S no passo 2.

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

$$
\begin{aligned}
(x_0, y_0) &= v_1 P + v_2 Q \\
&= H(m) A^{-1} P + R A^{-1} Q \\
&= A^{-1} (H(m) P + R Q) \\
&= A^{-1} (H(m) P + RsP) \\
&= A^{-1} (H(m) + Rs) P \\
&= k_2 (H(m) + Rs)^{-1} (H(m) + Rs) P \\
&= k_2 P
\end{aligned}
$$

$V = x_0 = x_1 = R.$

9. Uma forma de tentar obter o S é:

~~Encontra~~

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