/ /

UFRJ - Universidade Federal do Rio de Janeiro

Rio de Janeiro, 06 de Junho de 2017

- COMPONENTES (ALGORITMOS) BÁSICOS DE UM SISTEMA DE CRIPTOGRAFIA DE CHAVE PÚBLICA:

1) Geração do par de chaves
↳ Destinatário

Chave pública → Encriptação (remetente)
Chave privada → Decriptação (destinatário)

2) Encriptação
↳ Remetente

3) Decriptação
↳ Destinatário

- SEGURANÇA: Dificuldade computacional de se calcular a chave privada a partir do conhecimento apenas dos dados públicos.

- RSA:

1) Geração das chaves:

ENTRADA: dois primos distintos p e q

SAÍDA: chave pública (n, e) e chave privada (n, d)

INSTRUÇÕES:

1) Calcule $n = p \cdot q$

2) Calcule $\phi(n) = (p-1)(q-1)$

3) Busco e no intervalo $1 < e < \phi(n) = 1$ (e tem inverso módulo $\phi(n)$)

4) Calculo d, o inverso de e módulo $\phi(n)$ ($ed \equiv 1 \pmod{\phi(n)}$), utilizando o algoritmo Euclidiano Estendido

5) Retorno (n, e) como chave pública e (n, d) como chave privada

2) Encriptação

ENTRADA: Chave pública (n, e) e um bloco b tal que $1 < b < n$.

SAÍDA: bloco encriptado b'.

INSTRUÇÕES:

1) Retorne a forma reduzida de b^e módulo n (utilizando o algoritmo de potenciação modular).

3) Decriptação

ENTRADA: chave privada (n, d) e um bloco encriptado b' tal que $1 < b' < n$.

SAÍDA: bloco decriptado b'

INSTRUÇÕES:

1) Retorne a forma reduzida de $(b')^d$ módulo n. (utilizando o algoritmo de potenciação modular)

- SEGURANÇA DO RSA: Para calcular a chave privada a partir da chave pública, um dos passos necessários é a fatoração de n, o que é muito difícil computacionalmente no caso geral.

- EL GAMAL:

↳ Inventado pelo egípcio Taher El Gamal em 1985

⇒ Sistema de criptografia de chave pública baseado em grupos cíclicos

1) Geração do par de chaves

1.1) Seleciono um primo p.

1.2) Iremos trabalhar no grupo $U(p)$

$U(p) = \{1, 2, \dots, p-1\} = \mathbb{Z}_p - \{0\}$

1.3) Pelo teorema da raiz primitiva, $U(p)$ é garantidamente cíclico.

1.4) A ordem de $U(p)$ é $p-1$. Logo, como $U(p)$ é cíclico, $U(p)$ tem $\phi(p-1)$ geradores

1.5) Selecionados um gerador g de $U(p)$. (Uma maneira é utilizar o algoritmo de Gauss)

$U(p) = \{1, g, g^2, g^3, \dots, g^{p-2}\}$

1.6) Seleciono um inteiro a no intervalo $1 \leq a \leq p-1$

1.7) Calculo c = forma reduzida de g^a módulo p $(c \equiv g^a \pmod p)$

1.8) Os valores g e p são divulgados como parâmetros públicos (são utilizados tanto na encriptação quanto na decriptação)

1.9) A chave pública é o valor c

1.10) A chave privada é o valor a.

- SEGURANÇA: Para "quebrar" o sistema, preciso ser capaz de calcular o valor privado a a partir dos valores públicos c, g e p. Mas, estes quatro satisfazem a relação $g^a \equiv c \pmod p$, logo, para calcular a, preciso ser capaz de encontrar a solução para o problema do logaritmo discreto ($g^x \equiv c \pmod p$). Este problema é computacionalmente muito difícil.

2) Encriptação:

2.1) O bloco b a ser encriptado precisa estar no intervalo $1 < b < p-1$

2.2) Para encriptar um bloco, preciso sortar aleatóriamente um valor de K no intervalo $1 < K < p-1$

2.3) Preciso sortear um novo sorteio aleatório de K para cada bloco que vou encriptar.

2.4) Caso se utilize o mesmo valor de K para encriptar vários blocos distintos, isto pode ser explorado para quebrar a criptografia de forma eficiente.

2.5) Calculo s = forma reduzida do g^K módulo p ($s \equiv g^K \pmod p$)

2.6) Calculo t = forma reduzida do $b \cdot c^K$ módulo p ($t \equiv b \cdot c^K \pmod p$)

2.7) A encriptação do bloco b é o par (s, t)

- VANTAGEM DO EL GAMAL SOBRE O RSA: Precisa de apenas um primo ao invés de dois

/ /

- VANTAGEM DO RSA SOBRE O EL GAMAL: O tamanho do bloco encriptado é o mesmo do bloco original. Já no El Gamal, o tamanho é o dobro.

OBSERVAÇÃO: Como K é usado em apenas um bloco ele é "jogado fora" logo após o cálculo de s e t. K é conhecido como chave efêmera

3) Decriptação:

3.1) Recebo um bloco encriptado (s, t)

3.2) Conheço os valores de g e p.

3.3) Possuo a chave privada a

3.4) Calculo $s' \equiv (s)^{p-1-a} \pmod p$

3.5) Calculo $b = s' \cdot t \pmod p$

3.6) Este b é igual ao bloco original (antes de ser encriptado)

- POR QUE FUNCIONA?

- ENCRIPTAÇÃO:

Bloco b

$s \equiv g^{K} \pmod p$

$t \equiv b \cdot c^{K} \pmod p$

- DECRIPTAÇÃO:

$$s' \equiv (s)^{p-1-a} \pmod{p}$$

$$b' \equiv s' \cdot t \pmod{p}$$

- QUERO MOSTRAR QUE:

$$b' = b$$

$$s' \equiv s^{p-1-a} \equiv (g^k)^{p-1-a} \equiv g^{k(p-1)-ak} \pmod{p}$$

$$\begin{aligned}
b' &\equiv s' t \equiv g^{k(p-1)-ak} \cdot t \equiv \\
&\equiv g^{k(p-1)-ak} \cdot b \cdot c^k \equiv \\
&\equiv g^{k(p-1)-ak} \cdot b \cdot (g^a)^k \equiv \\
&\equiv g^{k(p-1)-ak} \cdot b \cdot g^{ak} \equiv \\
&\equiv g^{k(p-1)-ak} \cdot g^{ak} \cdot b \equiv \\
&\equiv g^{k(p-1)\cancel{-ak+ak}} \cdot b \equiv \\
&\equiv g^{k(p-1)} \cdot b \equiv (\underset{\underset{1}{\equiv}}{g^{p-1}})^k \cdot b \equiv b \pmod{p}
\end{aligned}$$

$$\left.\begin{array}{l} b' \equiv b \pmod{p} \\ 1 < b' < p \\ 1 < b < p \end{array}\right\} b' = b$$

EXEMPLO:

$p = 127$

$g = 3$

$a = 10$

$c = g^a \equiv 3^{10} \equiv 121 \pmod{127}$

$b = 42$

$k = 5$

$s = g^k \equiv 3^5 \equiv 116 \pmod{127}$

$t \equiv b \cdot c^k \equiv 42 \cdot 121 \equiv 52 \pmod{127}$

$(s,t) = (116, 52)$

Decriptação:

$s' \equiv s^{p-1-a} \equiv 116^{127-1-10} \equiv 116^{116} \equiv 35 \pmod{127}$

$b' \equiv s' \cdot t \equiv 35 \cdot 52 \equiv 42 \pmod{127}$