Pelotas/RS, *Junho 2020*

Métodos Criptográficos

Cleber Peter

clebers.peter@sou.ucpel.edu.br

Universidade Católica de Pelotas (UCPEL)

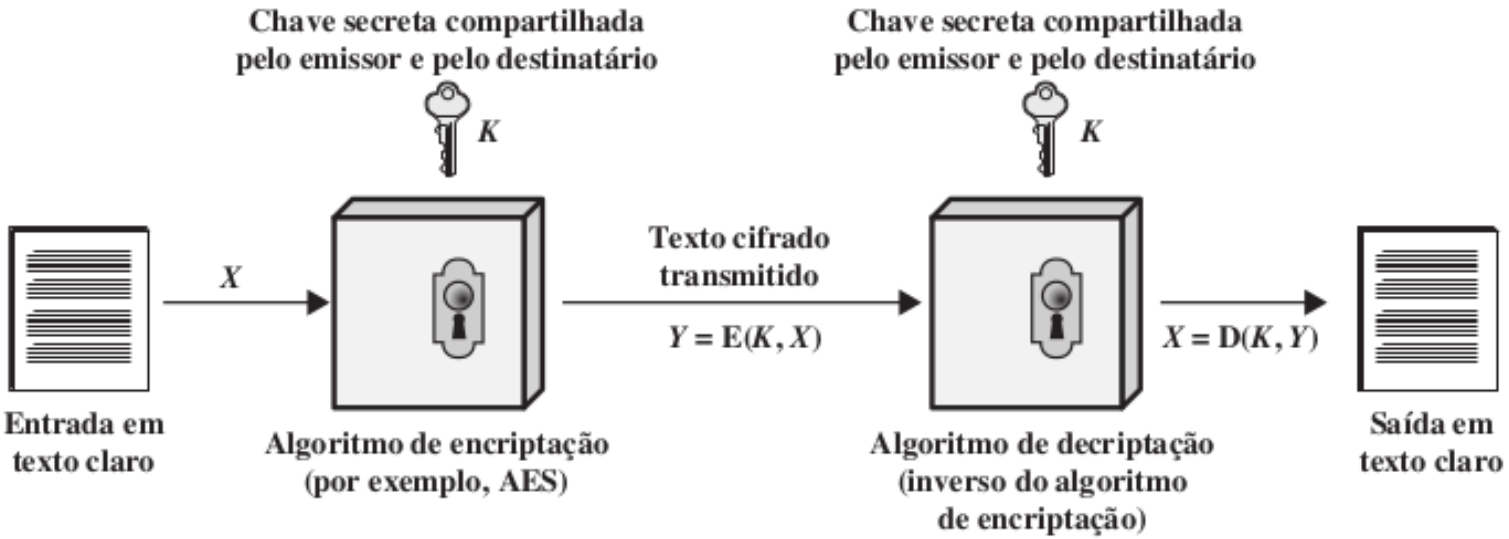
Roteiro

- Introdução
- Criptografia Simétrica
- Criptografia Assimétrica
- Demonstração TLS
- Conclusão

Criptografia

Conceito

Campo de estudo que define métodos e técnicas para a escrita de mensagens em forma cifrada ou em código, isto é, que se tornem inintelígiveis à terceiros.



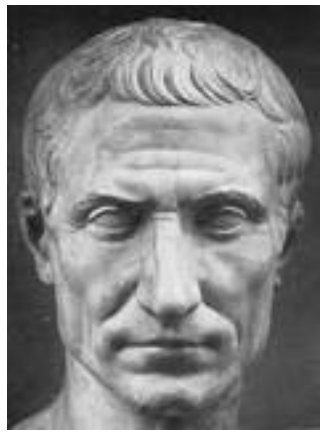
Cifra de César

Método criptográfico mais antigo de que se tem notícia atribuído ao imperador romano Júlio César.

```
claro: meet me after the toga party
cifra: PHHW PH DIWHU WKH WRJD SDUWB
```

$$C = E(k, p) = (p + k) \; mod \; 26$$

$$p = D(k, C) = (C - k) \; mod \; 26$$



Advanced Encryption Standard (AES)

Cifra simétrica de bloco proposta pelo Institute of Standards and Techonology (NIST) em 2001 para substituição do (DES, 1977).

Características

- Processa o texto claro em blocos de 128 bits;
- O tamanho da chave é variável (AES-128, AES-192 ou AES-256);
- Utiliza **aritmética de corpo finito** $GF(2^8)$.

Aritmética de Corpo Finito

No AES todas as operações são realizadas em 8 bits (1 byte), mais especificamente sobre corpos finitos GF(2^8) – *Galois Field*.

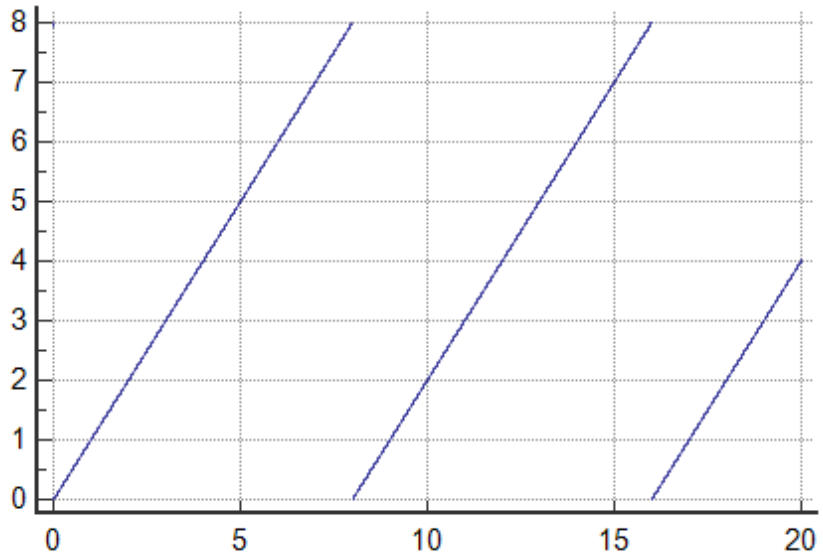
Corpo

Um conjunto em que as operações aritméticas de **soma, subtração, multiplicação e divisão** entre membros do conjunto sempre resultam noutro membro deste conjunto. $\mathbb{R}$ é um exemplo de corpo infinito.

Aritmética Modular - Corpos Finitos

$$a \bmod n = r$$

* Mapeia todos os números no conjunto $\{0, 1, ..., n-1\}$.



Corpo - Requisitos

Soma

Todos os termos do conjunto a_i devem possuir um **inverso aditivo** b_i também membro do conjunto tal que:

$$(a_i + b_i)\ mod\ n = 0$$

Divisão ($a/b = a * b^{-1}$)

Todos os termos do conjunto a_i devem possuir um **inverso multiplicativo** b_i também membro do conjunto tal que:

$$(a_i * b_i)\ mod\ n = 1$$

Aritmética em GF(7)

$$n = 7,\ a = b = \{0, 1, \ldots, 6\}$$

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

(a) Adição módulo 7

×	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

(b) Multiplicação módulo 7

w	$-w$	w^{-1}
0	0	–
1	6	1
2	5	4
3	4	5
4	3	2
5	2	3
6	1	6

(c) Inversos aditivo e multiplicativo módulo 7

Aritmética em GF(8)

$$n = 8,\ a = b = \{0, 1, \ldots, 7\}$$

+	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

(a) Adição módulo 8

×	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

(b) Multiplicação módulo 8

w	$-w$	w^{-1}
0	0	—
1	7	1
2	6	—
3	5	3
4	4	—
5	3	5
6	2	—
7	1	7

(c) Inverso aditivo e multiplicativo módulo 8

Inverso Multiplicativo

Constatações

- Existe um inverso multiplicativo b_i para um termo a_i, se e somente se, a_i for relativamente primo de n.
- Para garantir que todos os termos sejam relativamente primos de n é necessário que n seja um **número primo**.

Problemas

Restringir a escolha de n a um número primo é um desperdício de recursos o mais próximo de 256 é 251.

Aritmética de Polinômios Modular

Objetivo

Definir um corpo $GF(p^n)$ para n **não primo** e $p = 2$.

$$f(x) = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1x + a_0 = \sum_{i=0}^{n-1} a_i x^i$$

$a_i = \{0, 1, ..., p-1\}$. Existem p^n polinômios. Para $n = 3$:

0	$x+1$	x^2+x
1	x^2	x^2+x+1
x	x^2+1	

Redefinição das Operações Aritméticas

- A aritmética sobre os coeficientes é realizada GF(2), isto é:

$$(a_i.b_i)\ mod\ 2 = c_i$$

- Se a multiplicação resultar em um polinômio com grau maior que n-1, ele deve ser reduzido módulo algum polinômio irredutível m(x) de grau n, isto é:

$$r(x) = f(x)\ mod\ m(x)$$

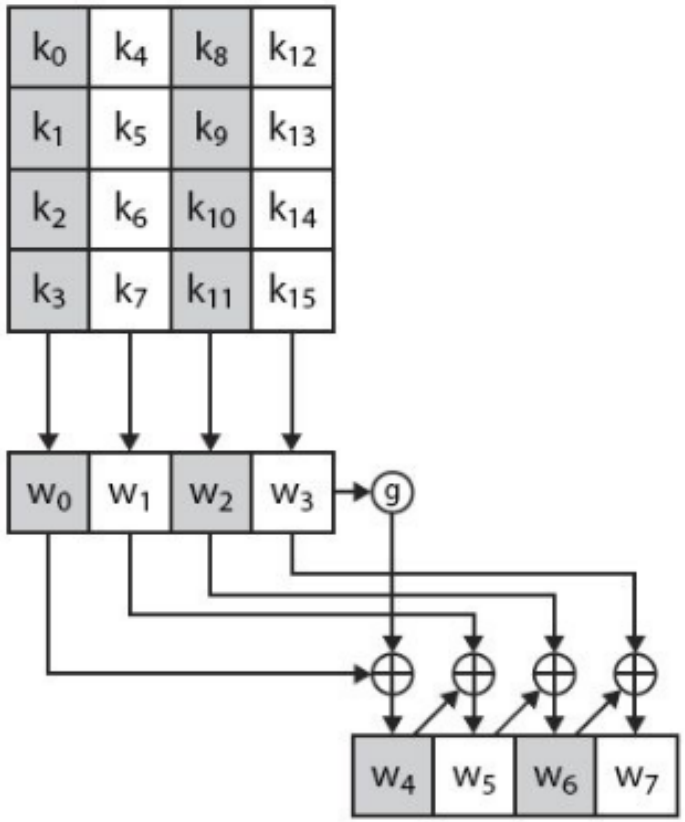
Multiplicação $GF(2^3)$

Para um polinômio irredutível $m(x) = x^3 + x + 1$:

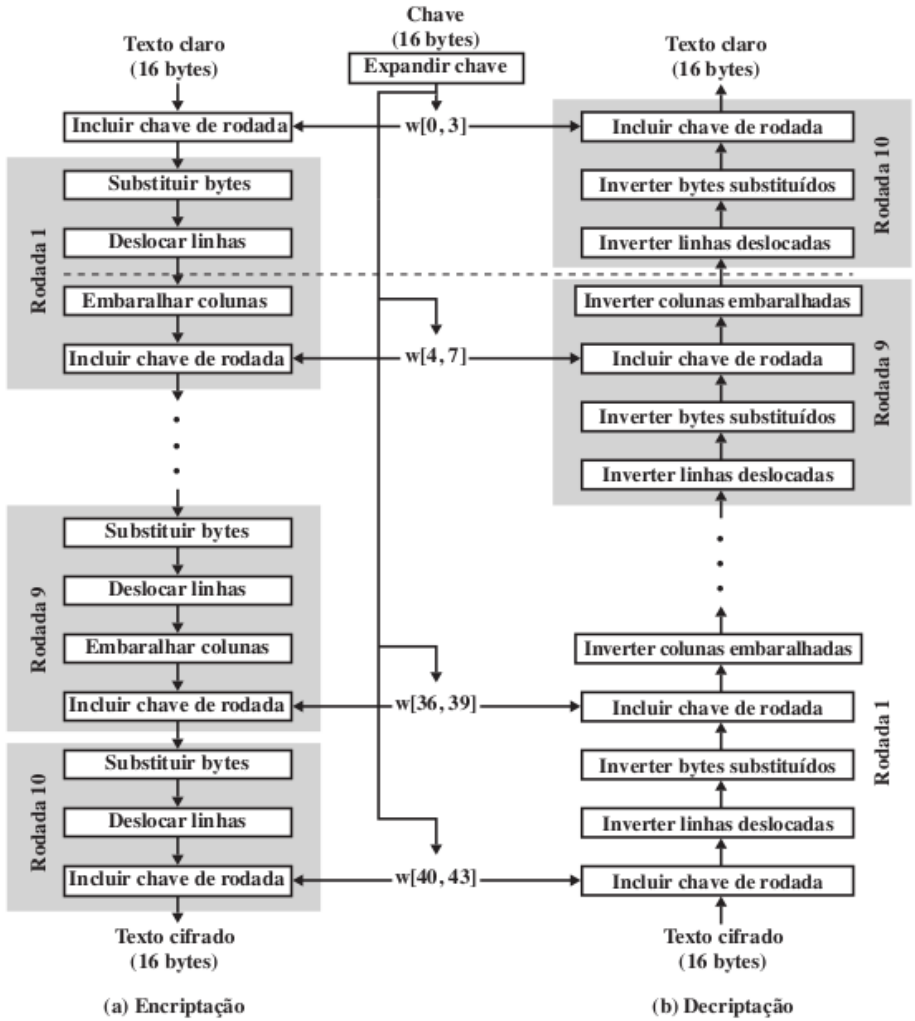
×	000 0	001 1	010 x	011 $x+1$	100 x^2	101 x^2+1	110 x^2+x	111 x^2+x+1
0	0	0	0	0	0	0	0	0
1	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
x	0	x	x^2	x^2+x	$x+1$	1	x^2+x+1	x^2+1
$x+1$	0	$x+1$	x^2+x	x^2+1	x^2+x+1	x^2	1	x
x^2	0	x^2	$x+1$	x^2+x+1	x^2+x	x	x^2+1	1
x^2+1	0	x^2+1	1	x^2	x	x^2+x+1	$x+1$	x^2+x
x^2+x	0	x^2+x	x^2+x+1	1	x^2+1	$x+1$	x	x^2
x^2+x+1	0	x^2+x+1	x^2+1	x	1	x^2+1	x^2	$x+1$

O AES utiliza $GF(2^8)$ e $m(x) = x^8 + x^4 + x^3 + x + 1$ como polinômio irredutível.

Expansão de Chave do AES-128



Estrutura do AES-128



Criptografia Assimétrica

Conceito revolucionário proposto por Diffie e Hellman em 1976 para resolver o problema da **distribuição de chaves**.

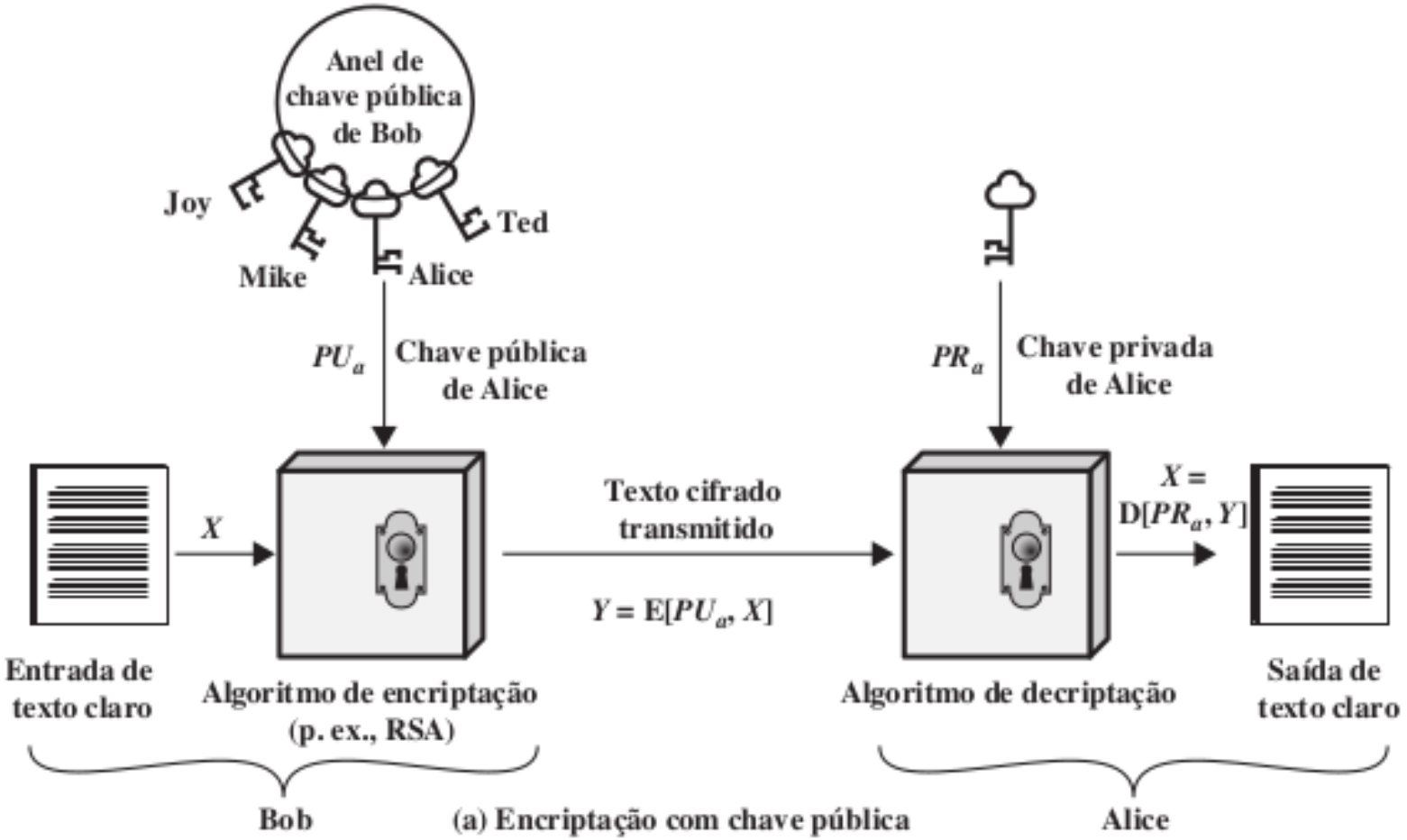
Estratégia

Existem duas chaves: uma pública (PBK) e outra privada (PRK).

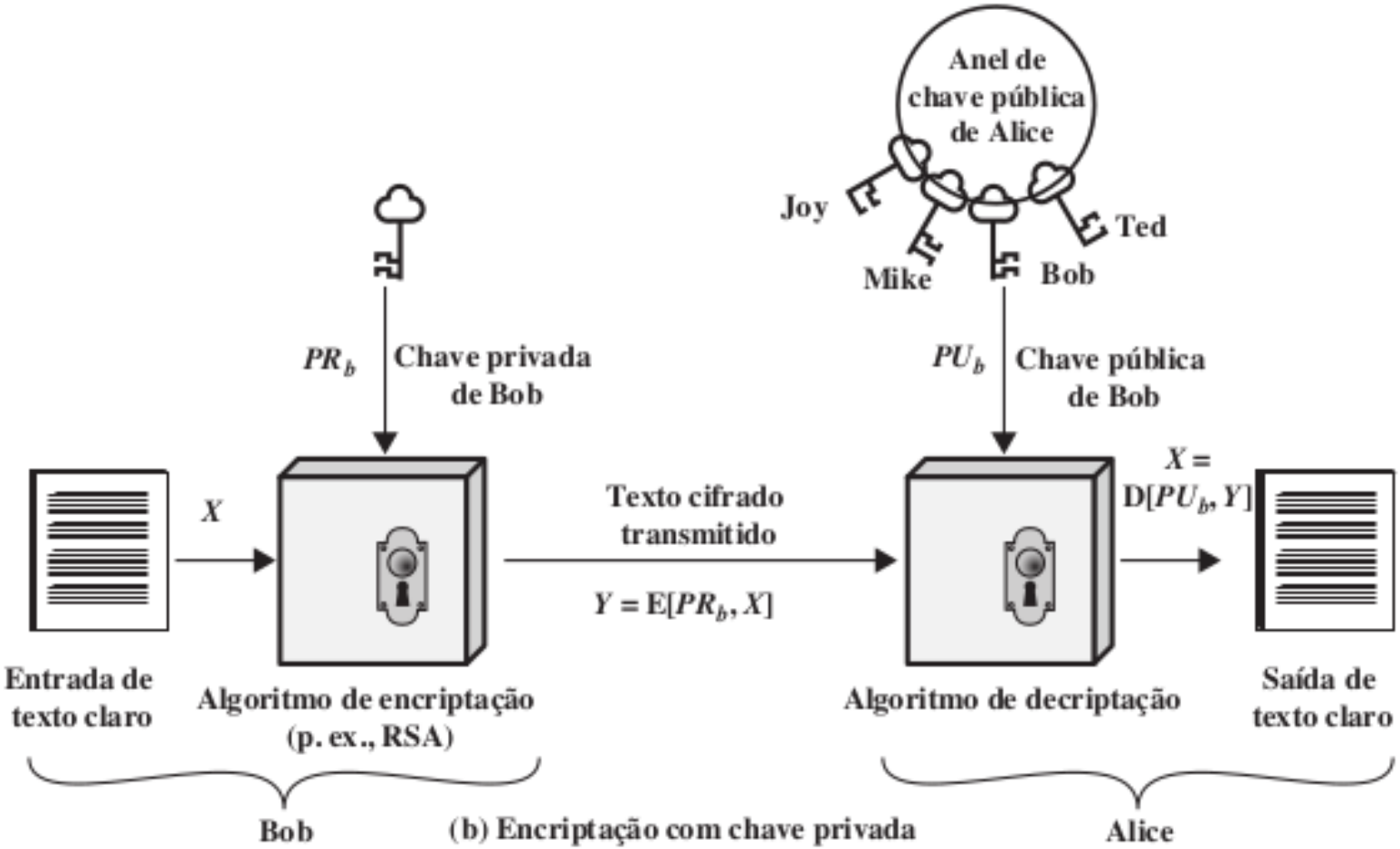
Requisitos

- Algo encriptado com PBK só pode ser decriptado pela PRK e vice-versa.
- A partir da PBK não é possível deduzir a PRK.

Confidencialidade



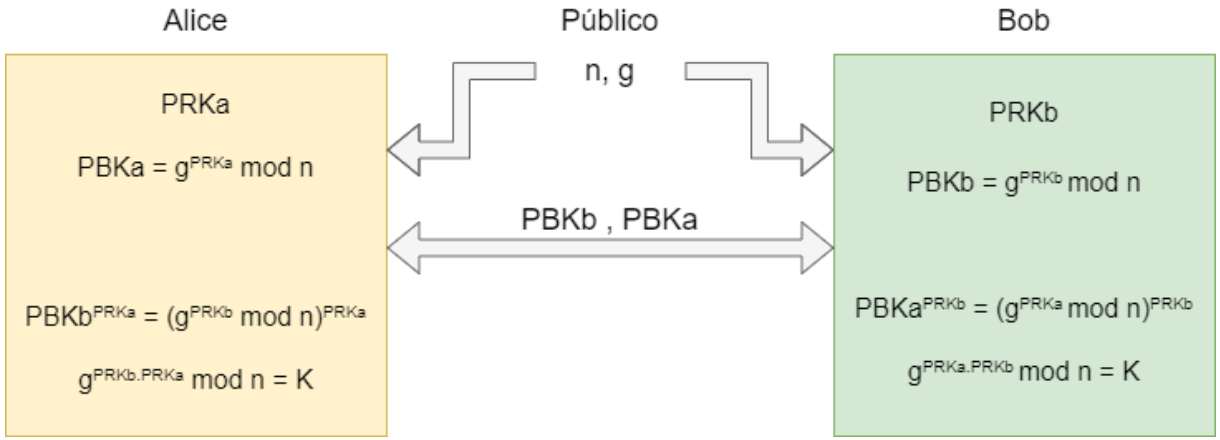
Autenticidade



Troca de Chaves Diffie-Hellman

Requisitos

- n: número primo de 1024 bits (309 dígitos);
- g: número primo normalmente 2 ou 5;
- PRKa, PRKb: número natural gerado randomicamente.



Logaritmos Discretos

A segurança deste método está vinculada a dificuldade de se obter PRK_x dado g, n e PBK_x.

$$PBK_x = g^{\mathbf{PRK_x}} \; mod \; n$$

O algoritmo mais rápido conhecido para solução do logaritmo discreto possui complexidade:

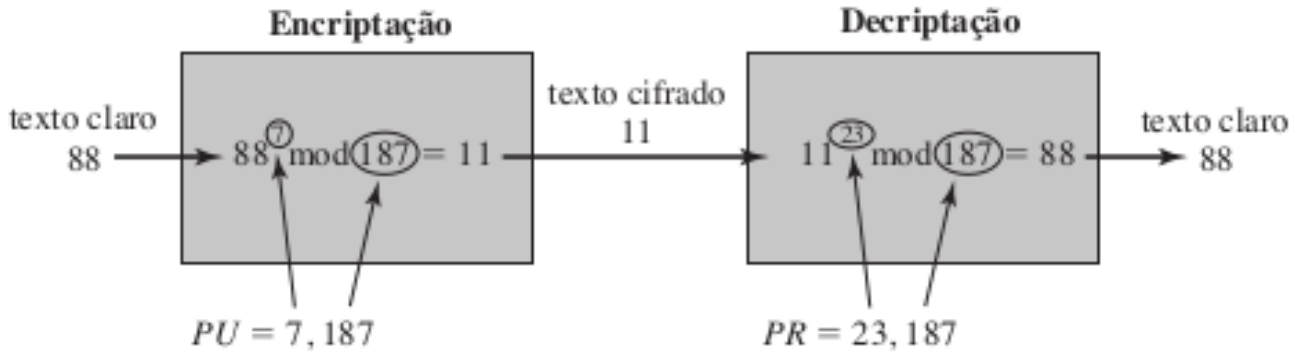
$$e^{((\ln n)^{1/3}(ln(\ln n))^{2/3})}$$

RSA

Atua sobre o texto claro em blocos de 2^n bits, foi proposto no MIT em 1978 por Ron Rivest, Adi Shamir e Len Adleman.

$$C = M^{PBKx} \ mod \ n$$

$$C^{PRKx} = M^{PBKx.PRKx} \ mod \ n = M$$



Geração do Par de Chaves RSA

- São escolhidos dos primos aleatórios grandes **p** e **q**;
- É calculado: $n = p * q$
- É calculado: $\phi(n) = (p-1) * (q-1)$
- $\boldsymbol{PBK_x}$: $1 < PBK_x < \phi(n)$ e $mdc(PBK_x, \phi(n)) = 1$
- $\boldsymbol{PRK_x}$: $\boldsymbol{PRK_x} * PBK_x \equiv 1 \; mod \; \phi(n)$

+ RSA

Segurança

- Esta relacionada a dificuldade de fatorar os dois números primos grandes p e q que resultam em n.
- Atualmente utiliza-se um n com pelo menos 617 dígitos decimais ocupando **2048 bits** de memória.

```
RSA-2048 = 25195908475657893494027183240048398571429282126204032027777137836043662020707
           59555626401852588078440691829064124951508218929855914917618450280848912007 2
           84499268739280728777673597141834727026189637501497182469116507761337985909 57
           00097330459748808428401797429100642458691817195118746121515172654632282216 86
           99875491824224336372590851418654620435767984233871847744479207399342365848 23
           82428119816381501067481045166037730605620161967625613384414360383390441495 26
           34432190114657544454178424020924616515723350778707749817125772467962926386 35
           63732899121548314381678998850404453640235273819513786365643912120103971228 22
           120720357
```

Criptografia de Curva Elíptica (ECC)

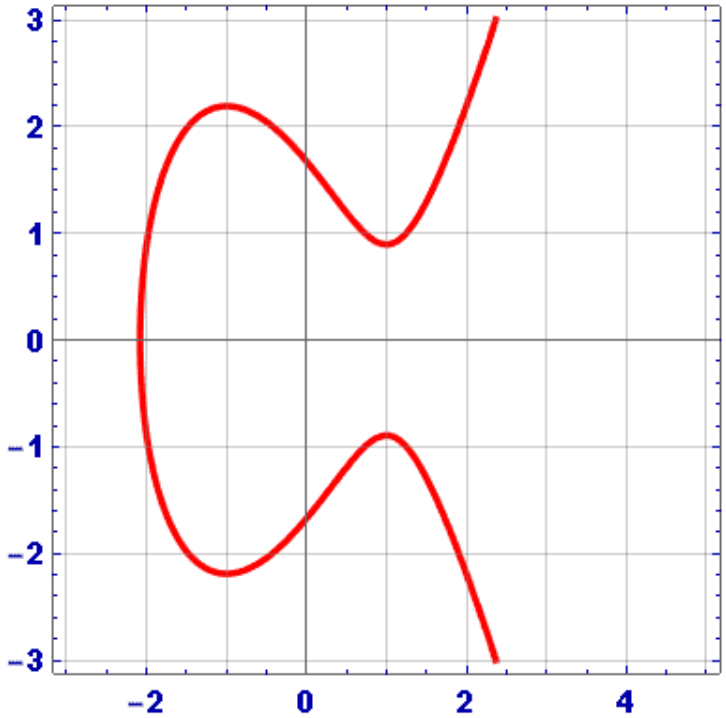
Proposto por Neal Koblitz e Victor S. Miller em 1985, porém teve seu uso aprovado pelo NIST somente em 2009 com o algoritmo (ECDSA).

Algoritmos

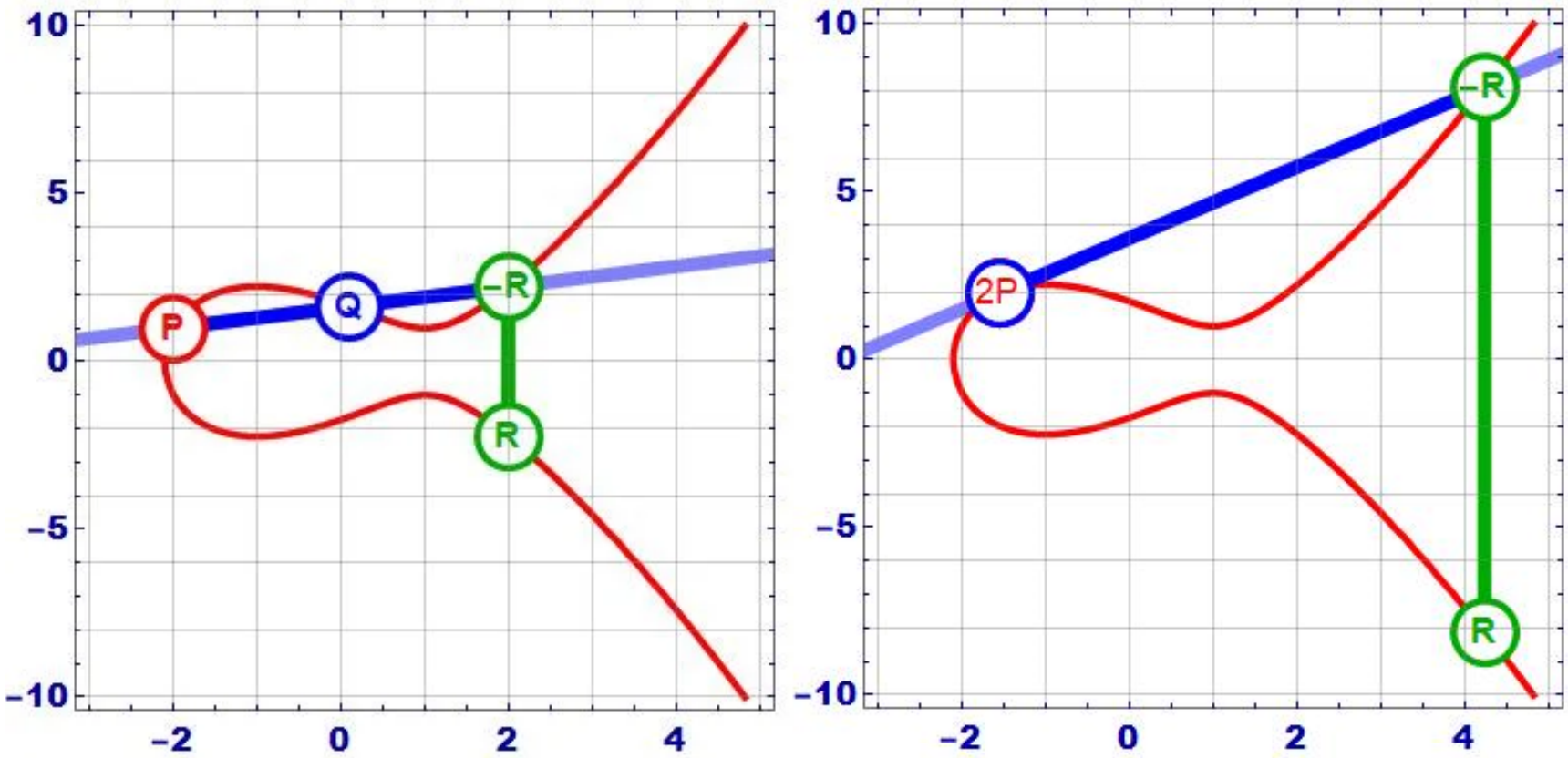
- ECDSA: Utilizado para **assinatura digital (Ethereum);**
- ECDH: Utilizado para **troca de chaves;**
- EdDSA: Utilizado para **assinatura digital (mais rápido).**

Curva Elíptica

$$y^2 = x^3 + Ax + B$$

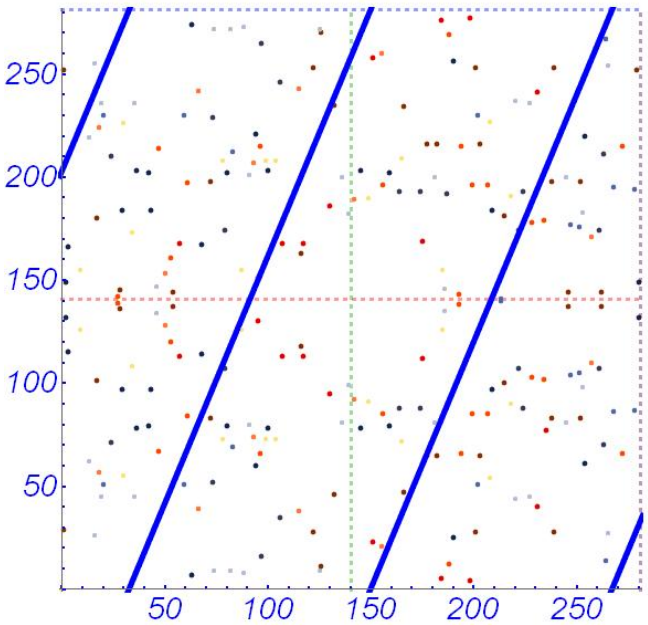


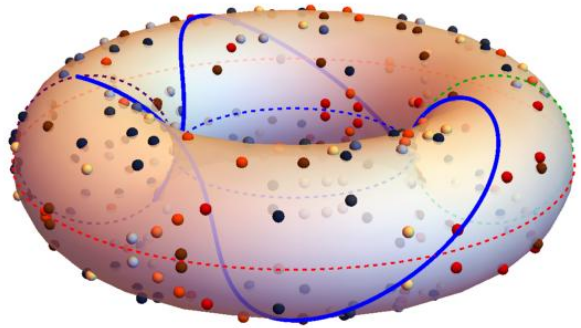
Curva Elíptica - Propriedades



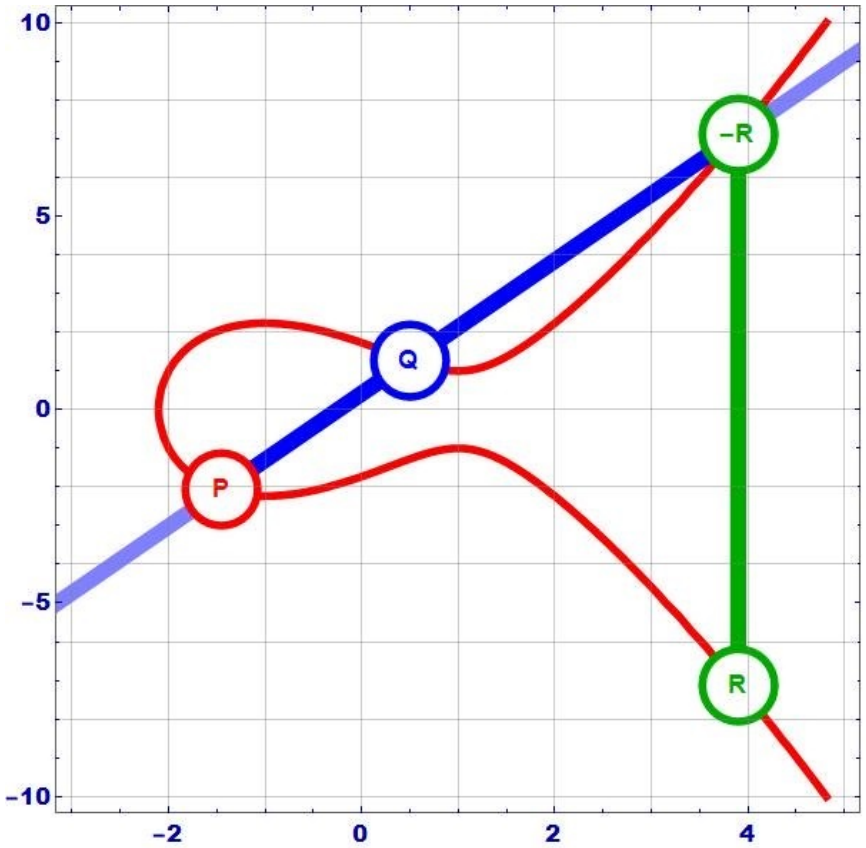
Curva Elíptica - Modular

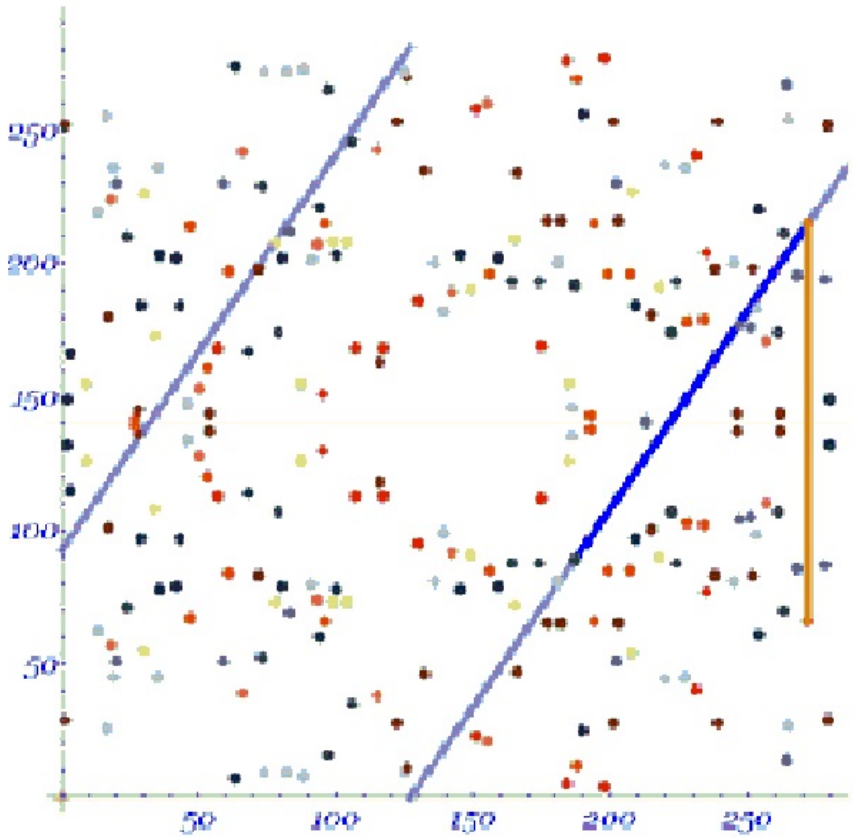
$$(y^2 - x^3 + 3x - 3) \; mod \; 281 = 0$$



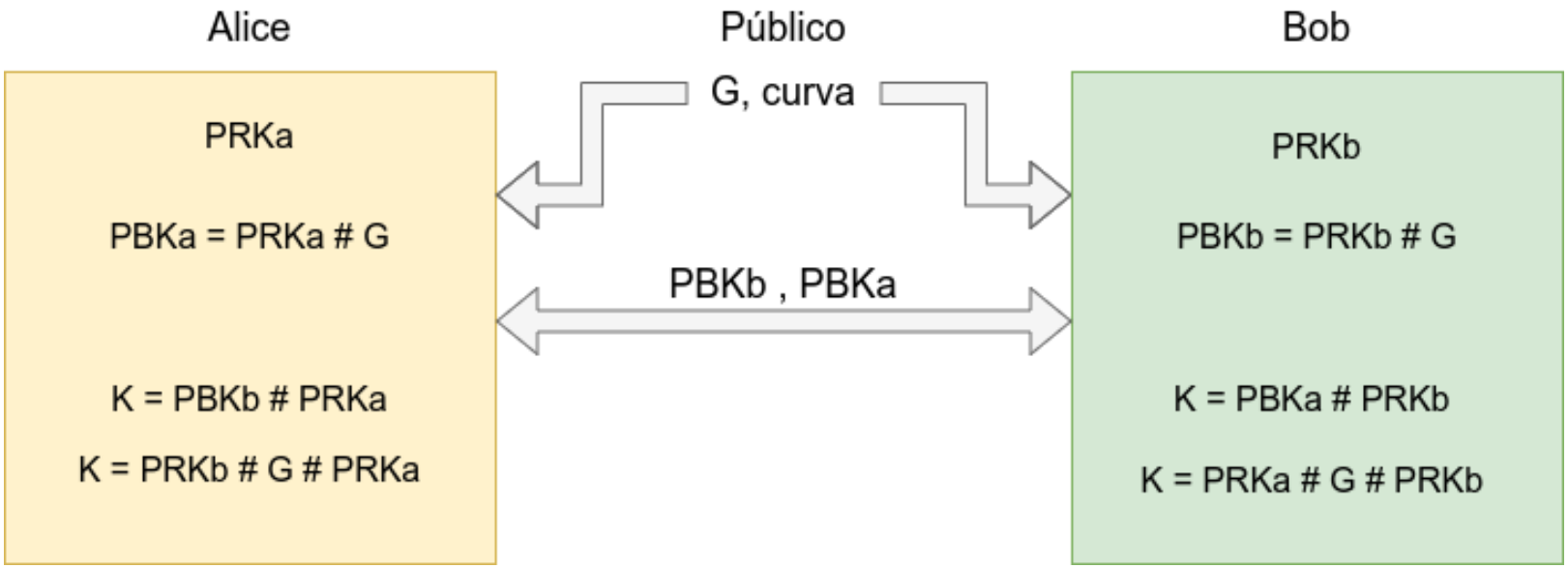


Curva Elíptica - Modular Soma





Eliptic Curve Diffie Helman (ECDH)



NIST Secp256k1 (Bitcoin)

$$y^2 - x^3 + 7 \equiv 0 \ (mod \ p)$$

$$p = 2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1$$

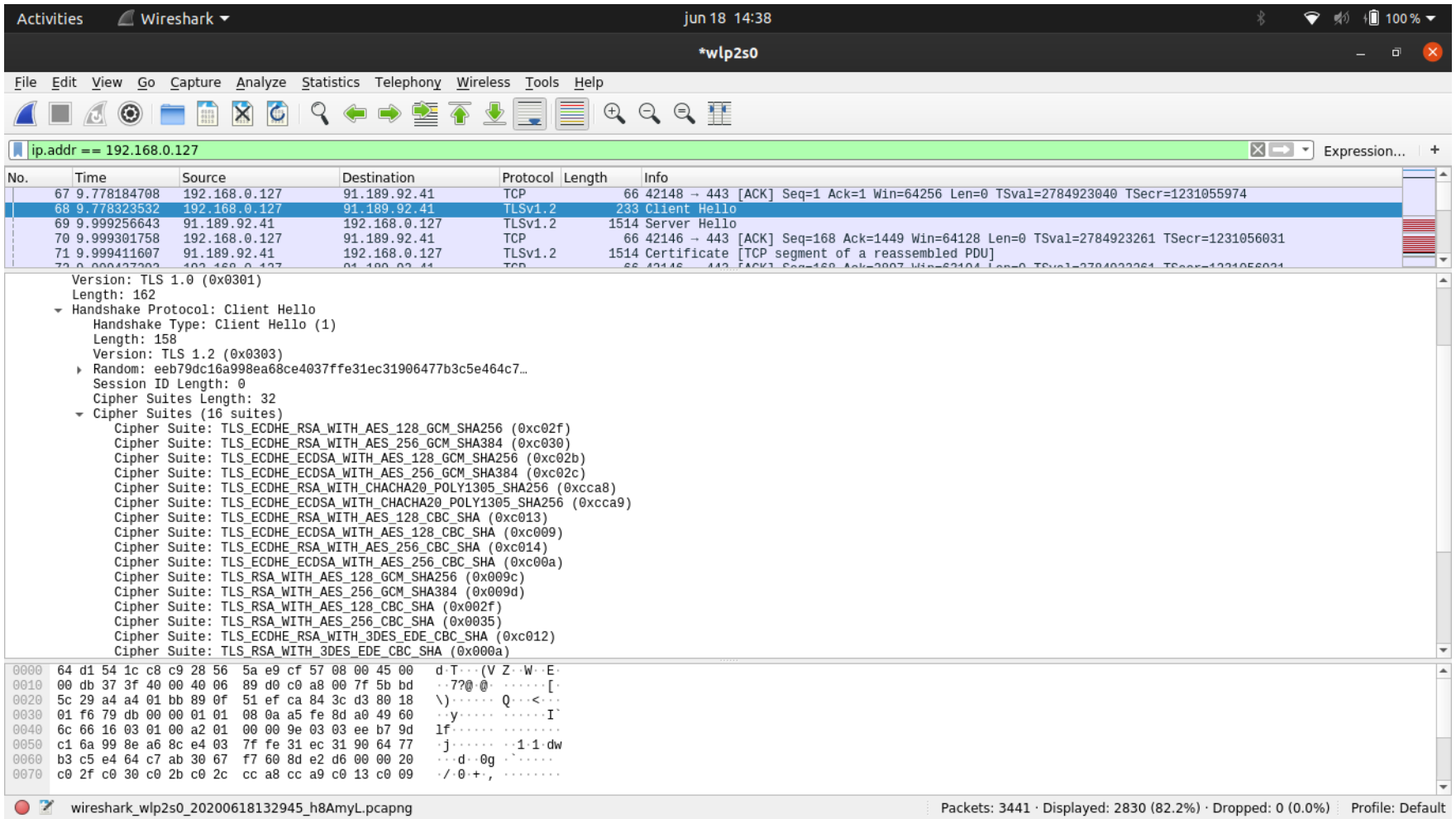
Segurança da ECC

- Obter o valor de $PBK_x = PRK_x * G$ é relativamente **rápido**, da ordem de $\log_2(PRKx)$.
- Porém obter $PRK_x = PBK_x/G$ é **impraticável** para PRK_x elevado. Conhecido como **problema do logaritmo discreto de curva elíptica (ECDLP).**
- Uma escolha adequada da curva e de seus parâmetros (G, PRK e etc) resulta em um ECDLP sem uma solução eficiente.

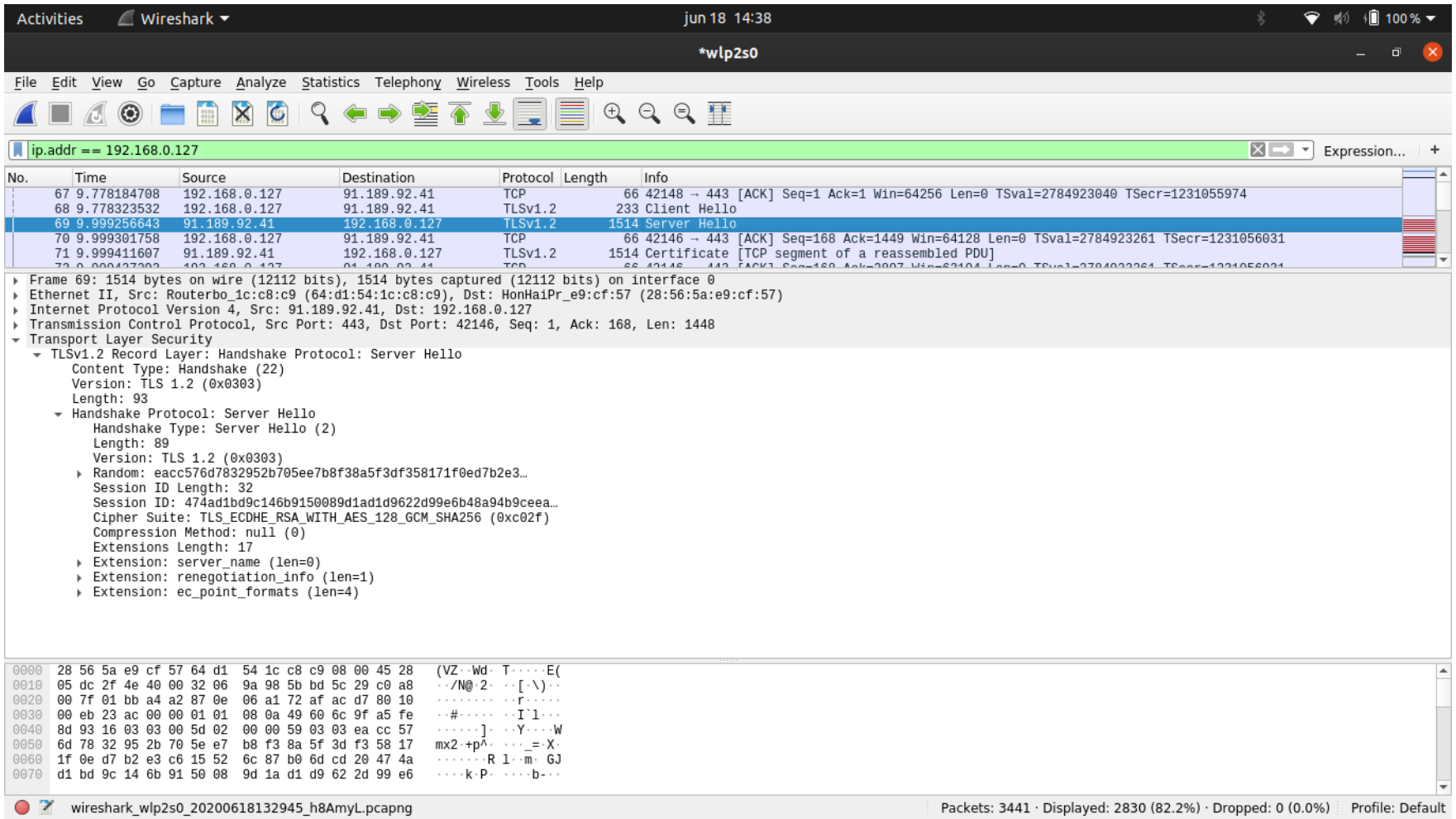
Recomendação NIST-2030

Key Type	Algorithms and Key Sizes
Digital Signature keys used for authentication (for Users or Devices)	RSA (2048 bits) ECDSA (Curve P-256)
Digital Signature keys used for non-repudiation (for Users or Devices)	RSA (2048 bits) ECDSA (Curves P-256 or P-384)
CA and OCSP Responder Signing Keys	RSA (2048 or 3072bits) ECDSA (Curves P-256 or P-384)
Key Establishment keys (for Users or Devices)	RSA (2048 bits) Diffie-Hellman (2048 bits) ECDH (Curves P-256 or P-384)

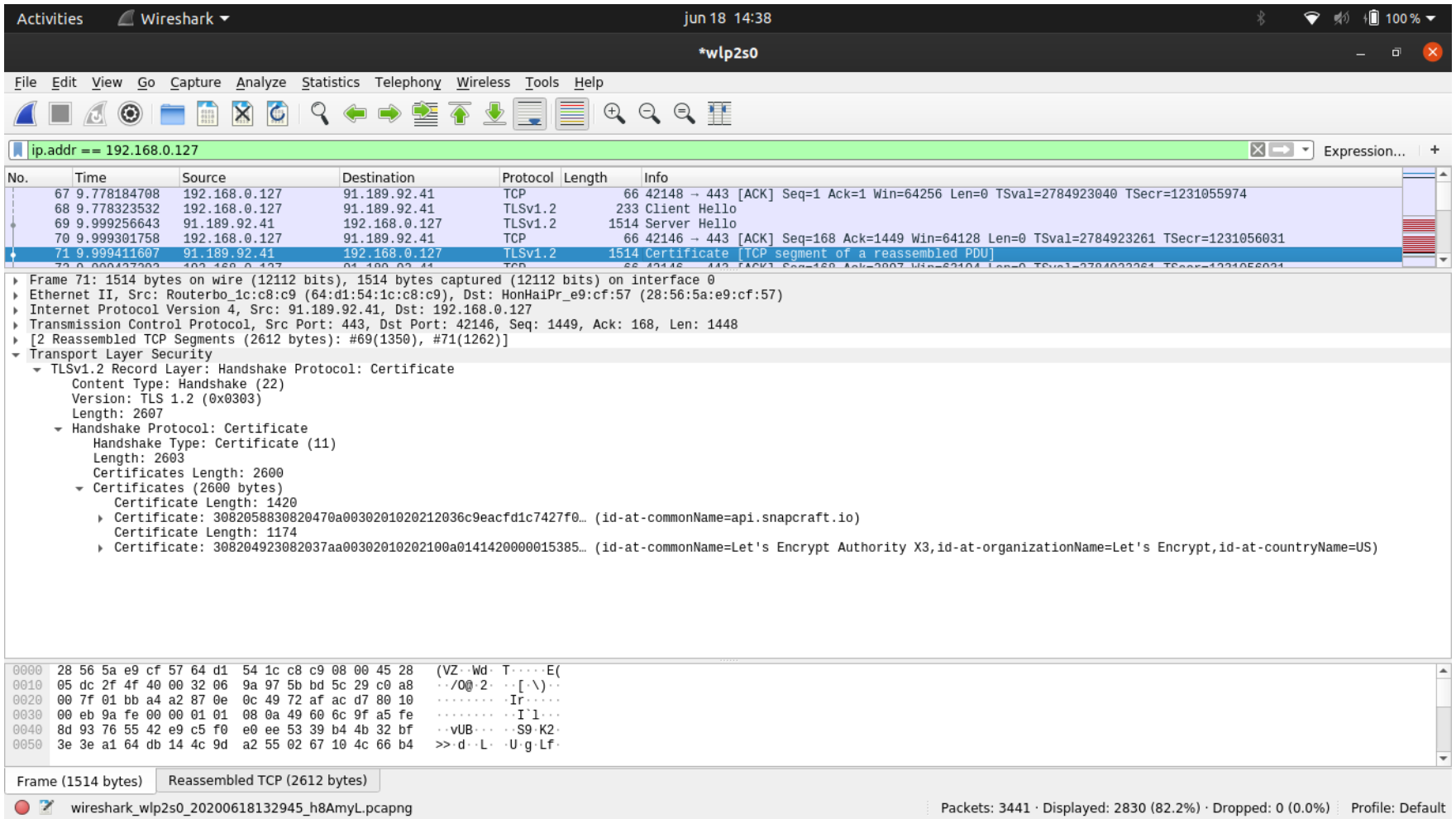
Vida Real? Transport Secure Layer (TLS)



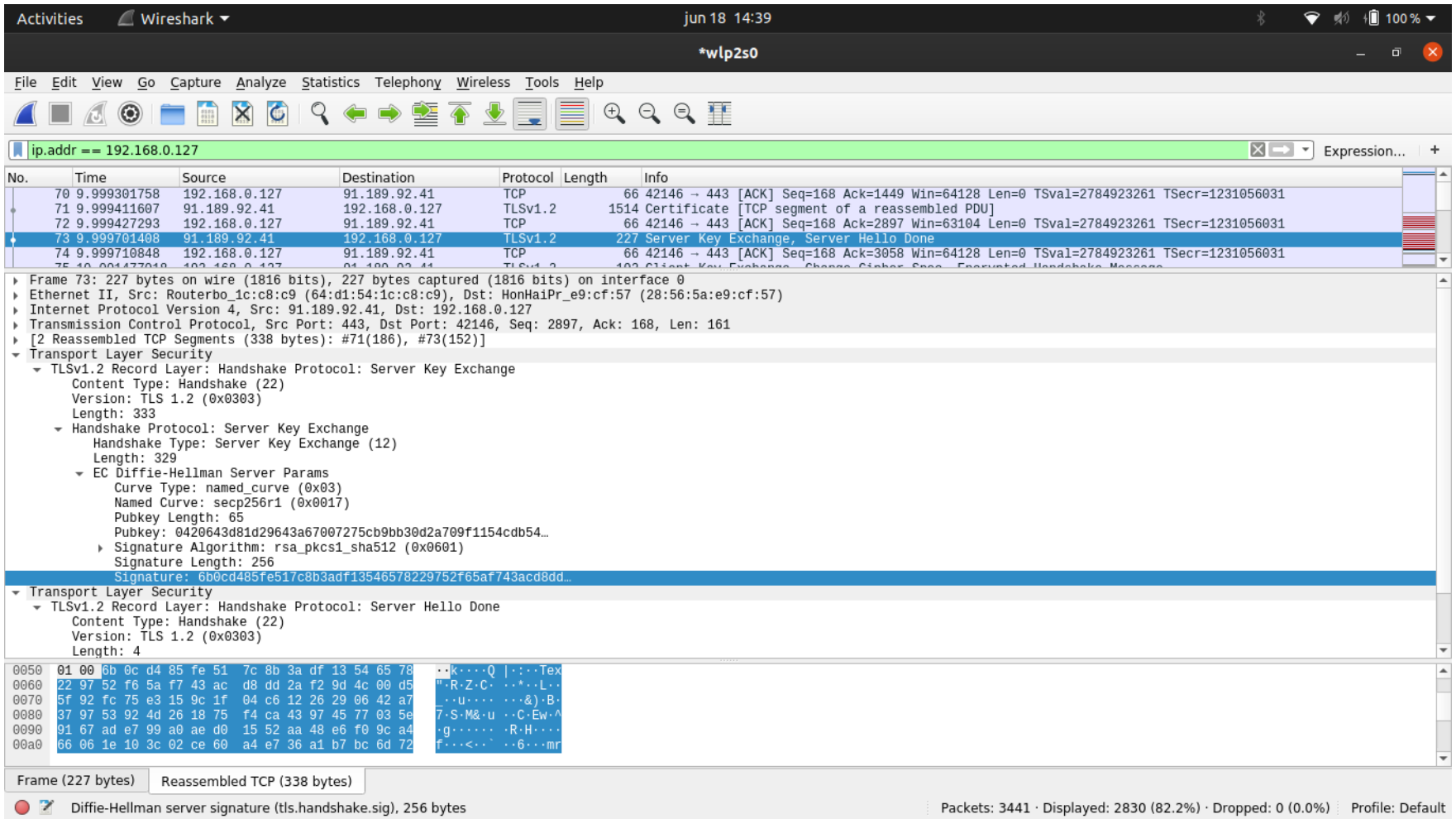
Definição da Cifra



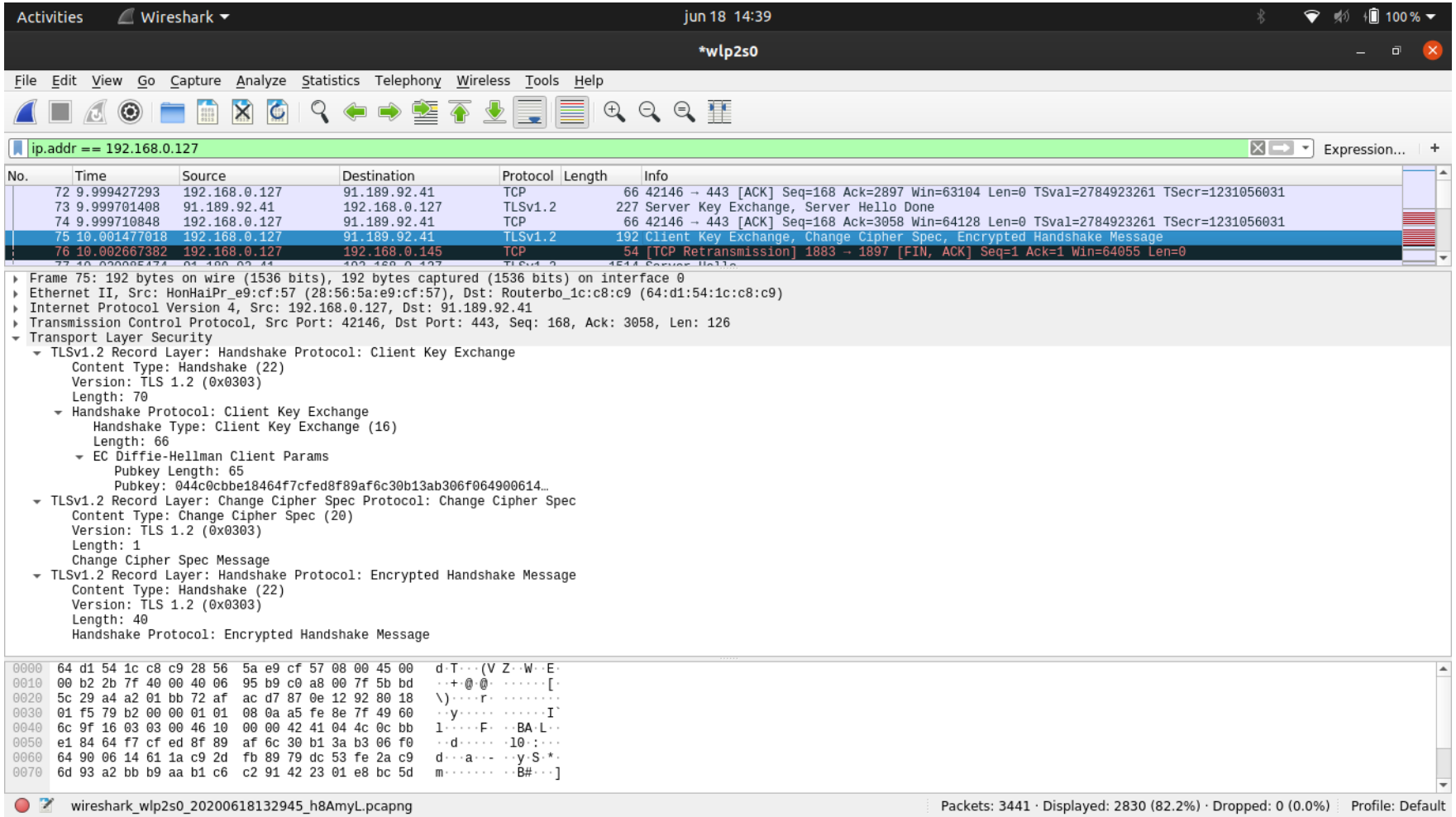
Envio do Certificado Digital



Compartilhamento de Chave Pública



Compartilhamento da Chave Pública



Futuro? Computadores Quânticos!

Previsões

- Na presença de computadores quânticos os algoritmos RSA e baseados em ECC (ECDSA, ECDH) **não são seguros.**
- As chaves utilizadas pelo AES precisarão ser maiores.

Solução

Em 2016 o NIST iniciou uma competição para selecionar algoritmos de criptografia assimétrica que sejam resistentes a computação quântica. **Ainda estão procurando :)**

Referências

William Stallings. 2010. **Cryptography and Network Security: Principles and Practice** *(5th. ed.). Prentice Hall Press, USA.*

Galbraith, S. (2012). **Mathematics of Public Key Cryptography**. *Cambridge: Cambridge University Press. doi:10.1017/CBO9781139012843*

Alagic, G., Alperin-Sheriff, J., Apon, D., Cooper, D., Dang, Q., Liu, Y.-K., Miller, C., Moody, D., Peralta, R., Perlner, R., Robinson, A., Smith-Tone, D. (2019). **Status report on the first round of the NIST post-quantum cryptography standardization process. National Institute of Standards and Technology**. *https://doi.org/10.6028/nist.ir.8240*

*Barker, E. B., Dang, Q. H. (2015).***Recommendation for Key Management Part 3: Application-Specific Key Management Guidance. National Institute of Standards and Technology**. *https://doi.org/10.6028/nist.sp.800-*

Brasil. **Portaria Instituto Nacional de Metrologia, Qualidade e Tecnologia - INMETRO nº 559**, *de 15 de dezembro de 2016*