

Pelotas/RS, Junho 2020



Métodos Criptográficos

Cleber Peter

✉ clebers.peter@sou.ucpel.edu.br

🏛 Universidade Católica de Pelotas (UCPEL)

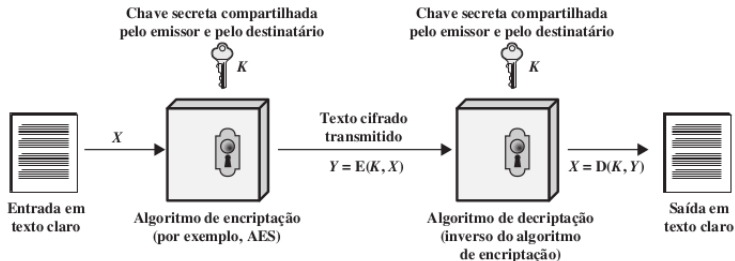
Roteiro

- 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 ininteligíveis 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

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

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



Advanced Encryption Standard (AES)

Cifra simétrica de bloco proposta pelo Institute of Standards and Technology (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*.

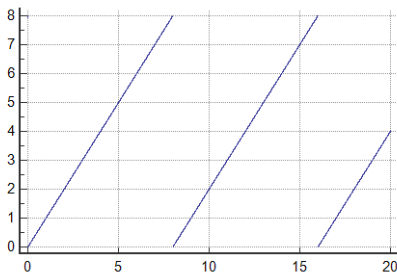
Corpo

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 $\{0, 1, \dots, n - 1\}$.



Corpo - Requisitos

Soma

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

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

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:

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

Aritmética em GF(7)

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

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

(c) Inversos aditivo e multiplicativo módulo 7

Aritmética em GF(8)

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

+	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

x	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 $p = 2$.

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

$a_i = \{0, 1, \dots, p-1\}$. 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:

$$(a_i \cdot b_i) \bmod 2 = c_i$$

- ▶ 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:

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

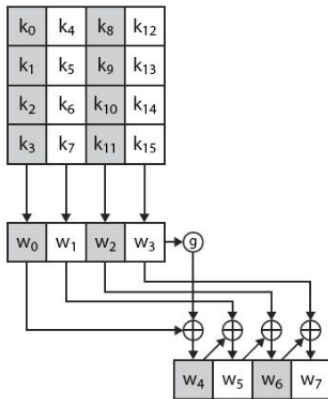
Multiplicação $GF(2^3)$

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

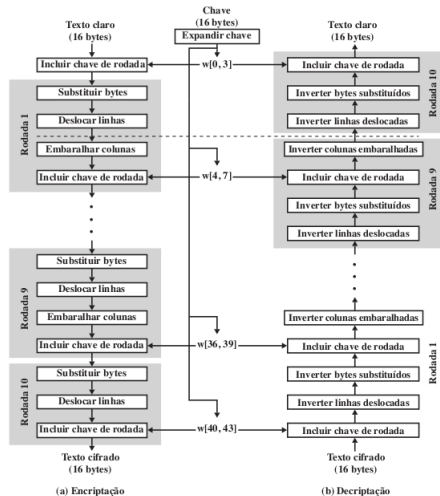
	000	001	010	011	100	101	110	111
$\times$	0	1	x	$x + 1$	x^2	$x^2 + 1$	$x^2 + x$	$x^2 + x + 1$
0	0	0	0	0	0	0	0	0
1	0	1	x	$x + 1$	x^2	$x^2 + 1$	$x^2 + x$	$x^2 + x + 1$
x	0	x	x^2	$x^2 + x$	$x + 1$	1	$x^2 + x + 1$	$x^2 + 1$
$x + 1$	0	$x + 1$	$x^2 + x$	$x^2 + 1$	$x^2 + x + 1$	x^2	1	x
x^2	0	x^2	$x + 1$	$x^2 + x + 1$	$x^2 + x$	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 irreduzível.

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**.

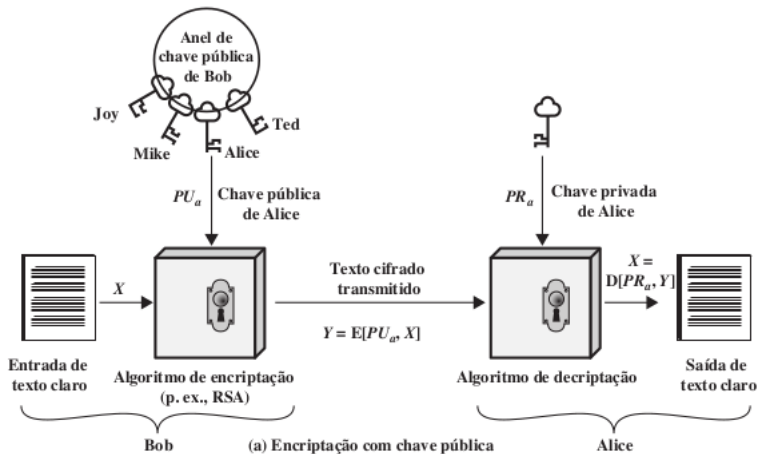
Estratégia

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

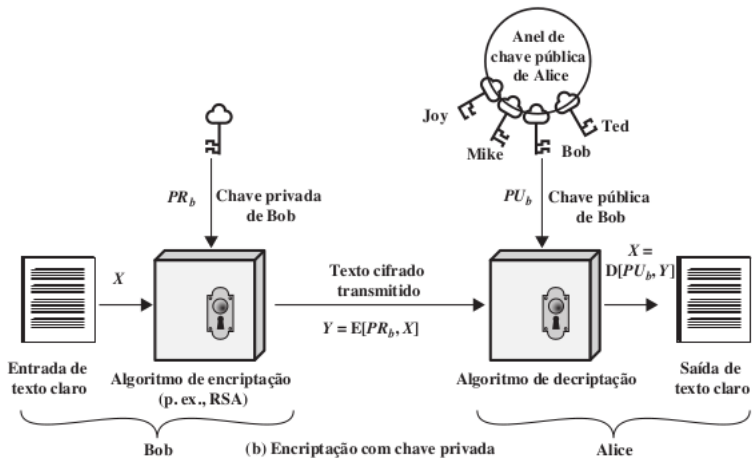
Requisitos

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

Confidencialidade



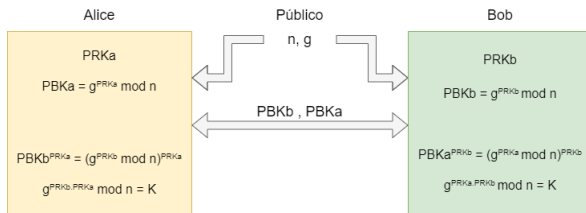
Autenticidade



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 .

$$PBK_x = g^{PRK_x} \bmod n$$

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

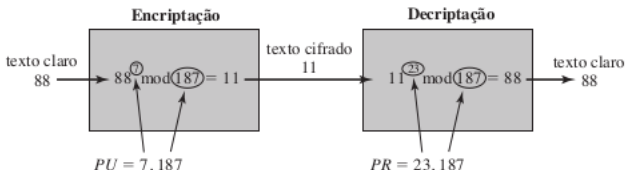
$$e^{((\ln n)^{1/3} (\ln(\ln n))^{2/3})}$$

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.

$$C = M^{PBK_x} \bmod n$$

$$C^{PRK_x} = M^{PBK_x \cdot PRK_x} \bmod n = M$$



Geração do Par de Chaves RSA

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

+ 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 = 2519590847565789349402718324004839857142928212620403202777713783604366202070
7595556264018525880784406918290641249515082189298559149176184502808489120072
8449926873928072877767359714183472702618963750149718246911650776133798590957
0009733045974880842840179742910064245869181719511874612151517265463228221686
9987549182422433637259085141865462043576798423387184774447920739934236584823
8242811981638150106748104516603773060562016196762561338441436038339044149526
3443219011465754445417842402092461651572335077870774981712577246796292638635
6373289912154831438167899885040445364023527381951378636564391212010397122822
120720357
```


Criptografia de Curva Elíptica (ECC)

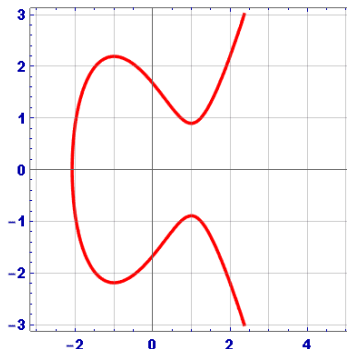
Proposto por Neal Koblitz e Victor S. Miller em 1985, porém teve seu uso aprovado pelo NIST somente em 2009 com o algoritmo (ECDSA).

Algoritmos

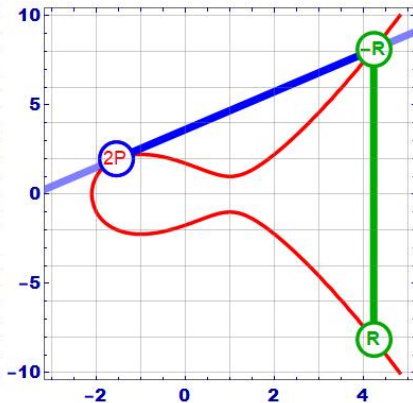
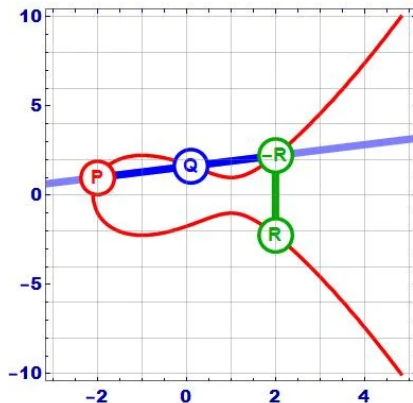
- ▶ ECDSA: Utilizado para **assinatura digital (Ethereum)**;
- ▶ ECDH: Utilizado para **troca de chaves**;
- ▶ EdDSA: Utilizado para **assinatura digital (mais rápido)**.

Curva Elíptica

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

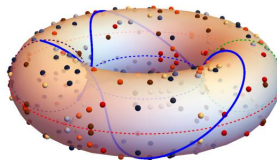
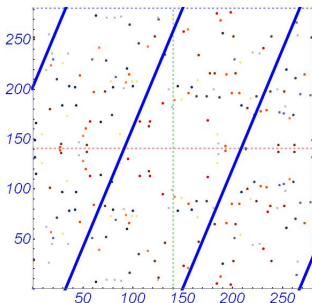


Curva Elíptica - Propriedades

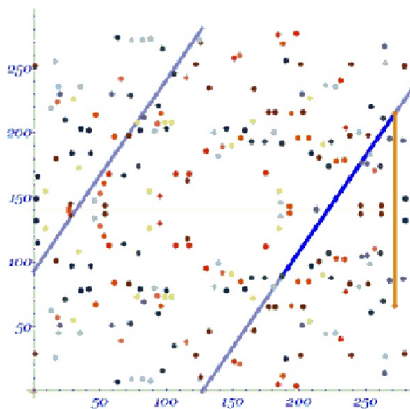
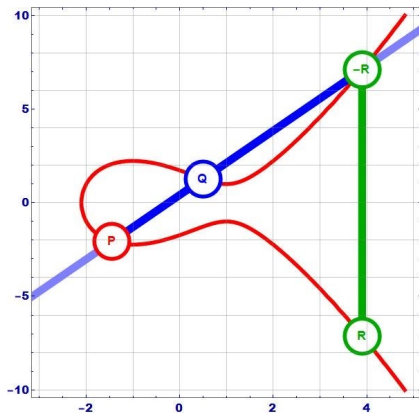


Curva Elíptica - Modular

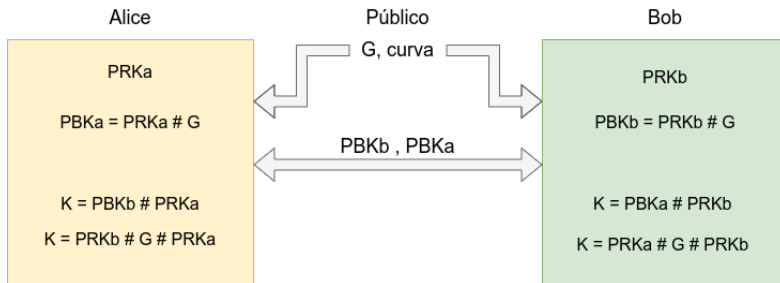
$$(y^2 - x^3 + 3x - 3) \bmod 281 = 0$$



Curva Elíptica - Modular Soma



Elliptic Curve Diffie Helman (ECDH)



NIST Secp256k1 (Bitcoin)

$$y^2 - x^3 + 7 \equiv 0 \pmod{p}$$

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

Segurança da ECC

- ▶ Obter o valor de $PBK_x = PRK_x * G$ é relativamente **rápido**, da ordem de $\log_2(PRK_x)$.
- ▶ 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)

Activities Wireshark jun 18 14:38 *wlp2s0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 192.168.0.127

No.	Time	Source	Destination	Protocol	Length	Info
67	9.778184788	192.168.0.127	192.168.0.127	TCP	66	42148 -> 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2784923040 TSecr=1231055974
68	9.778321332	192.168.0.127	192.168.0.127	TLSv1.2	732	Client Hello
69	9.999256643	192.168.0.127	192.168.0.127	TLSv1.2	1514	Server Hello
70	9.999301758	192.168.0.127	192.168.0.127	TCP	66	42146 -> 443 [ACK] Seq=168 Ack=1449 Win=64128 Len=0 TSval=2784923261 TSecr=1231056031
71	9.999411687	192.168.0.127	192.168.0.127	TLSv1.2	1514	Certificate [TCP segment of a reassembled PDU]

Version: TLS 1.0 (0x0301)
 Length: 162
 Handshake Protocol: Client Hello
 Handshake Type: Client Hello (1)
 Length: 156
 Version: TLS 1.2 (0x0303)
 Random: eeb79dc16a990ea68ce4037ffe31ec31906477b3c5e464c7..
 Session ID Length: 0
 Cipher Suites Length: 32
 Cipher Suites (16 suites)
 Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
 Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
 Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
 Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)
 Cipher Suite: TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xc0a8)
 Cipher Suite: TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xc0a9)
 Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
 Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)
 Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
 Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)
 Cipher Suite: TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)
 Cipher Suite: TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)
 Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
 Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
 Cipher Suite: TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (0xc012)
 Cipher Suite: TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xc00a)

0000 64 d1 54 1c c8 29 56 5a e9 c7 57 08 00 45 0e d T...[V Z...M...E...
 0010 00 db 37 3f 40 00 40 06 89 d0 c0 a8 00 7f 5b bd 770 @[...
 0020 5c 29 a4 a4 01 bb 09 51 ef ca 84 3c d3 80 18 \).....Q...<...
 0030 01 f6 79 db 00 00 01 01 08 0a a5 fe 80 a0 49 60 y.....I...
 0040 6c 66 16 03 01 a2 01 00 90 9e 03 00 b7 9d If.....
 0050 c1 6a 99 8e a6 8c e4 03 7f fe 31 ec 31 90 64 7 j.....-11 dw
 0060 b3 c5 e4 64 c7 ab 30 67 f7 60 8d e2 d6 00 00 20 ..d..0g
 0070 c0 2f c0 30 c0 2b c0 2c cc a8 cc a9 c0 13 c0 09 / 0 +,

wireshark_wlp2s0_20200618132945_h8AmyL.pcapng

Packets: 3441 · Displayed: 2830 (82.2%) · Dropped: 0 (0.0%) · Profile: Default

Definição da Cifra

Activities Wireshark jun 18 14:38 *wlp2s0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 192.168.0.127 Expression...

No.	Time	Source	Destination	Protocol	Length	Info
67	9.778184788	192.168.0.127	91.189.92.41	TCP	66	42148 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2784923040 TSecr=1231055974
68	9.778323532	192.168.0.127	91.189.92.41	TLV1.2	233	Client Hello
69	9.779255741	91.189.92.41	192.168.0.127	TLV1.2	1514	Server Hello
70	9.999301758	192.168.0.127	91.189.92.41	TCP	66	42146 → 443 [ACK] Seq=168 Ack=1449 Win=64128 Len=0 TSval=2784923261 TSecr=1231056031
71	9.999411687	91.189.92.41	192.168.0.127	TLV1.2	1514	Certificate [TCP segment of a reassembled PDU]

Frame 69: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0

- Ethernet II, Src: Routerbo_1c:c8:c9 (64:d1:54:1c:c8:c9), Dst: MonMaiPr_e9:cf:57 (28:56:5a:e9:cf:57)
- Internet Protocol Version 4, Src: 91.189.92.41, Dst: 192.168.0.127
- Transmission Control Protocol, Src Port: 443, Dst Port: 42146, Seq: 1, Ack: 168, Len: 1448
- Transport Layer Security
 - TLV1.2 Record Layer: Handshake Protocol: Server Hello
 - Content Type: Handshake (22)
 - Version: TLS 1.2 (0x0303)
 - Length: 93
 - Handshake Protocol: Server Hello
 - Handshake Type: Server Hello (2)
 - Length: 89
 - Version: TLS 1.2 (0x0303)
 - Random: eacc576d7832952b705ee7b0f38a5f3df358171f0ed7b2e3..
 - Session ID Length: 32
 - Session ID: 474ad1bd9c146b9150089d1ad1d9622d99e6b48a94b9ccea..
 - Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
 - Compression Method: null (0)
 - Extensions Length: 17
 - Extension: server_name (len=0)
 - Extension: renegotiation_info (len=1)
 - Extension: ec_point_formats (len=4)

```

0000  28 56 5a e9 cf 57 64 d1 54 1c c8 c9 08 00 45 28  (VZ-Wd T....E(
0010  05 dc 2f 4e 40 80 32 06 9a 9c 5b bd 5c 29 c8 a8  ./N0 2:.-[.\)
0020  00 7f 01 bb a4 a2 87 0e 06 a1 72 af ac d7 80 10  .....-f.....
0030  00 eb 23 ac 00 00 01 01 08 0a 49 60 0c 9f a5 fe  ..#.....-I'...
0040  8d 93 16 83 63 6d 92 02 00 00 59 03 03 0a cc 57  .....-Y...W
0050  6d 78 32 95 2b 70 5e e7 b0 f3 8a 5f 3d f3 50 17  mx2+P^...=X.
0060  1f 0e d7 b2 e3 c6 15 52 6c 87 b0 6d cd 20 47 4a  ....R 1:m GJ
0070  d1 bd 9c 14 6b 91 50 08 9d 1a d1 d9 62 d4 99 e6  ....kP:....b...

```

wireshark_wlp2s0_20200618132945_h8AmyL.pcapng Packets: 3441 · Displayed: 2830 (82.2%) · Dropped: 0 (0.0%) Profile: Default

Envio do Certificado Digital

Activities Wireshark jun 18 14:38 *wlp2s0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 192.168.0.127

No.	Time	Source	Destination	Protocol	Length	Info
67	9.778184788	192.168.0.127	91.189.92.41	TCP	66	42148 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2784923040 TSecr=1231055974
68	9.778323532	192.168.0.127	91.189.92.41	TLSv1.2	233	Client Hello
69	9.999256643	91.189.92.41	192.168.0.127	TLSv1.2	1514	Server Hello
70	9.999301758	192.168.0.127	91.189.92.41	TCP	66	42146 → 443 [ACK] Seq=168 Ack=1449 Win=64128 Len=0 TSval=2784923261 TSecr=1231056031
71	9.999411697	91.189.92.41	192.168.0.127	TLSv1.2	1514	Certificate [TCP segment of a reassembled PDU]

Frame 71: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0
 Ethernet II, Src: Routerbo_1c:c8:c9 (64:d1:54:1c:c8:c9), Dst: MonMaiPr_e9:cf:57 (28:56:5a:e9:cf:57)
 Internet Protocol Version 4, Src: 91.189.92.41, Dst: 192.168.0.127
 Transmission Control Protocol, Src Port: 443, Dst Port: 42146, Seq: 1449, Ack: 168, Len: 1448
 2 Reassembled TCP Segments (2612 bytes): #69(1350), #71(1262)
 Transport Layer Security
 TLSv1.2 Record Layer: Handshake Protocol: Certificate
 Content Type: Handshake (22)
 Version: TLS 1.2 (0x0303)
 Length: 2607
 Handshake Protocol: Certificate
 Handshake Type: Certificate (11)
 Length: 2603
 Certificates Length: 2600
 Certificates (2600 bytes)
 Certificate Length: 1420
 Certificate: 3082058308920470a0030201020212036c9eacfd1c7427f0.. (id-at-commonName=api.snapcraft.io)
 Certificate Length: 1174
 Certificate: 308204923082037aa00302010202100a0141420000015385.. (id-at-commonName=Let's Encrypt Authority X3,id-at-organizationName=Let's Encrypt,id-at-countryName=US)

0000 28 56 5a e9 cf 57 64 d1 54 1c c8 c9 08 00 45 28 (VZ-Wd T....E(
 0010 05 dc 2f 4f 40 80 32 06 9a 97 5b bd 5c 29 c8 a8 ..0/2..[-\).
 0020 00 7f 01 bb a4 a2 87 0e 0c 49 72 af ac d7 80 19If.....
 0030 00 eb 9a fe 00 00 01 01 08 0a 49 60 6c 9f a5 feI'.....
 0040 0d 93 76 56 42 c5 f0 e0 e6 53 39 b4 4d 32 bf59K2.
 0050 3e 3e a1 64 db 14 4c 9d a2 55 02 67 10 4c 66 b4 >>d-L`U-gLf.

Frame (1514 bytes) Reassembled TCP (2612 bytes)

wireshark_wlp2s0_20200618132945_h8AmyL.pcapng

Packets: 3441 · Displayed: 2830 (82.2%) · Dropped: 0 (0.0%) · Profile: Default

Compartilhamento de Chave Pública

Activities Wireshark jun 18 14:39 *wlp250

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 192.168.0.127 Expression...

No.	Time	Source	Destination	Protocol	Length	Info
70	9.999301758	192.168.0.127	91.189.92.41	TCP	66	42146 → 443 [ACK] Seq=168 Ack=1449 Win=64128 Len=0 TSval=2784923261 TSecr=1231056031
71	9.999411687	91.189.92.41	192.168.0.127	TLSv1.2	1514	Certificate [TCP segment of a reassembled PDU]
72	9.999427293	192.168.0.127	91.189.92.41	TCP	66	42146 → 443 [ACK] Seq=168 Ack=2897 Win=63104 Len=0 TSval=2784923261 TSecr=1231056031
73	9.999701488	91.189.92.41	192.168.0.127	TLSv1.2	227	Server Key Exchange, Server Hello Done
74	9.999710848	192.168.0.127	91.189.92.41	TCP	66	42146 → 443 [ACK] Seq=168 Ack=3058 Win=64128 Len=0 TSval=2784923261 TSecr=1231056031

Frame 73: 227 bytes on wire (1816 bits), 227 bytes captured (1816 bits) on interface 0

- Ethernet II, Src: Routerbo-1c:c8:c9 (64:d1:54:1c:c8:c9), Dst: MonHaiPr-e9:cf:57 (28:56:5a:e9:cf:57)
- Internet Protocol Version 4, Src: 91.189.92.41, Dst: 192.168.0.127
- Transmission Control Protocol, Src Port: 443, Dst Port: 42146, Seq: 2897, Ack: 168, Len: 161
- 2 Reassembled TCP Segments (338 bytes): #71(186), #73(152)
- Transport Layer Security
 - TLSv1.2 Record Layer: Handshake Protocol: Server Key Exchange
 - Content Type: Handshake (22)
 - Version: TLS 1.2 (0x0303)
 - Length: 333
 - Handshake Protocol: Server Key Exchange
 - Handshake Type: Server Key Exchange (12)
 - Length: 329
 - EC Diffie-Hellman Server Params
 - Curve Type: named_curve (0x03)
 - Named Curve: secp256r1 (0x0017)
 - Pubkey Length: 65
 - Pubkey: 0420643081d29643a67007275cb0bb30d2a709f1154c0b54..
 - Signature Algorithm: rsa_pkcs1_sha512 (0x0601)
 - Signature Length: 256
 - Signature: 00c0485f51c0b3adf135465f8229f52f65af743acd80d...
 - Transport Layer Security
 - TLSv1.2 Record Layer: Handshake Protocol: Server Hello Done
 - Content Type: Handshake (22)
 - Version: TLS 1.2 (0x0303)
 - Length: 4

Frame (227 bytes) Reassembled TCP (338 bytes)

Diffie-Hellman server signature (tls.handshake.sig), 256 bytes

Packets: 3441 · Displayed: 2830 (82.2%) · Dropped: 0 (0.0%) · Profile: Default

Compartilhamento da Chave Pública

Activities Wireshark jun 18 14:39 *wlp2s0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 192.168.0.127

No.	Time	Source	Destination	Protocol	Length	Info
72	9.999427293	192.168.0.127	91.189.92.41	TCP	66	42146 → 443 [ACK] Seq=168 Ack=2897 Win=63104 Len=0 TSval=2784923261 TSecr=1231956031
73	9.999701488	91.189.92.41	192.168.0.127	TLsv1.2	227	Server Key Exchange, Server Hello Done
74	9.999719848	192.168.0.127	91.189.92.41	TCP	66	42146 → 443 [ACK] Seq=168 Ack=3958 Win=64128 Len=0 TSval=2784923261 TSecr=1231956031
75	10.001477818	192.168.0.127	91.189.92.41	TLsv1.2	192	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
76	10.002067382	192.168.0.127	192.168.0.149	TCP	54	[TCP Retransmission] 1883 → 1897 [FIN, ACK] Seq=1 Ack=1 Win=64055 Len=0

Frame 75: 192 bytes on wire (1536 bits), 192 bytes captured (1536 bits) on interface 0
 Ethernet II, Src: NonHwPr_e9:cf:57 (28:56:5a:e9:cf:57), Dst: Routerbo1c8:c9 (64:d1:54:1c:c8:c9)
 Internet Protocol Version 4, Src: 192.168.0.127, Dst: 91.189.92.41
 Transmission Control Protocol, Src Port: 42146, Dst Port: 443, Seq: 168, Ack: 3958, Len: 126
 Transport Layer Security
 TLsv1.2 Record Layer: Handshake Protocol: Client Key Exchange
 Content Type: Handshake (22)
 Version: TLS 1.2 (0x0303)
 Length: 70
 Handshake Protocol: Client Key Exchange
 Handshake Type: Client Key Exchange (16)
 Length: 66
 EC Diffie-Hellman Client Params
 Pubkey Length: 65
 Pubkey: 044c0cbb1846477cfe08f89a6c30b13ab306f864900514..

TLsv1.2 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
 Content Type: Change Cipher Spec (20)
 Version: TLS 1.2 (0x0303)
 Length: 1
 Change Cipher Spec Message

TLsv1.2 Record Layer: Handshake Protocol: Encrypted Handshake Message
 Content Type: Handshake (22)
 Version: TLS 1.2 (0x0303)
 Length: 40
 Handshake Protocol: Encrypted Handshake Message

0000 64 d1 54 1c c8 c9 28 56 5a e9 cf 57 08 00 45 00 d T...[V Z...W...E...
 0010 00 b2 2b 7f 40 00 40 06 95 b9 c0 a8 00 7f 5b bd + @ @[...
 0020 5c 29 a4 a2 81 bb 72 af ac d 87 0e 12 92 00 18 \).....r.....I...
 0030 01 f5 79 b2 00 00 01 01 08 0a a5 fe 86 7f 49 60 -y.....I...
 0040 6c 9f 16 03 00 40 06 10 00 80 42 41 04 4c 0c bb 1.....F...BA L...
 0050 e1 04 64 f7 cf ed 8f 89 af 6c 30 b1 3a b3 06 f0 d.....10 :...
 0060 64 90 06 14 61 1a c9 2d f0 80 79 dc 53 fe 2a c9 d.....y S *...
 0070 6d 93 a2 bb b9 aa b1 c6 c2 91 42 23 01 e8 bc 5d m.....B W...]

wireshark_wlp2s0_20200618132945_h8AmyL.pcapng

Packets: 3441 · Displayed: 2830 (82.2%) · Dropped: 0 (0.0%) · Profile: Default

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