CRIPTOGRAFIA

PROBLEMA DO LOGARITMO DISCRETO

Gonçalo Feliciano - 44292 | Joao Sampaio - 45749 - MIEI

SUMÁRIO

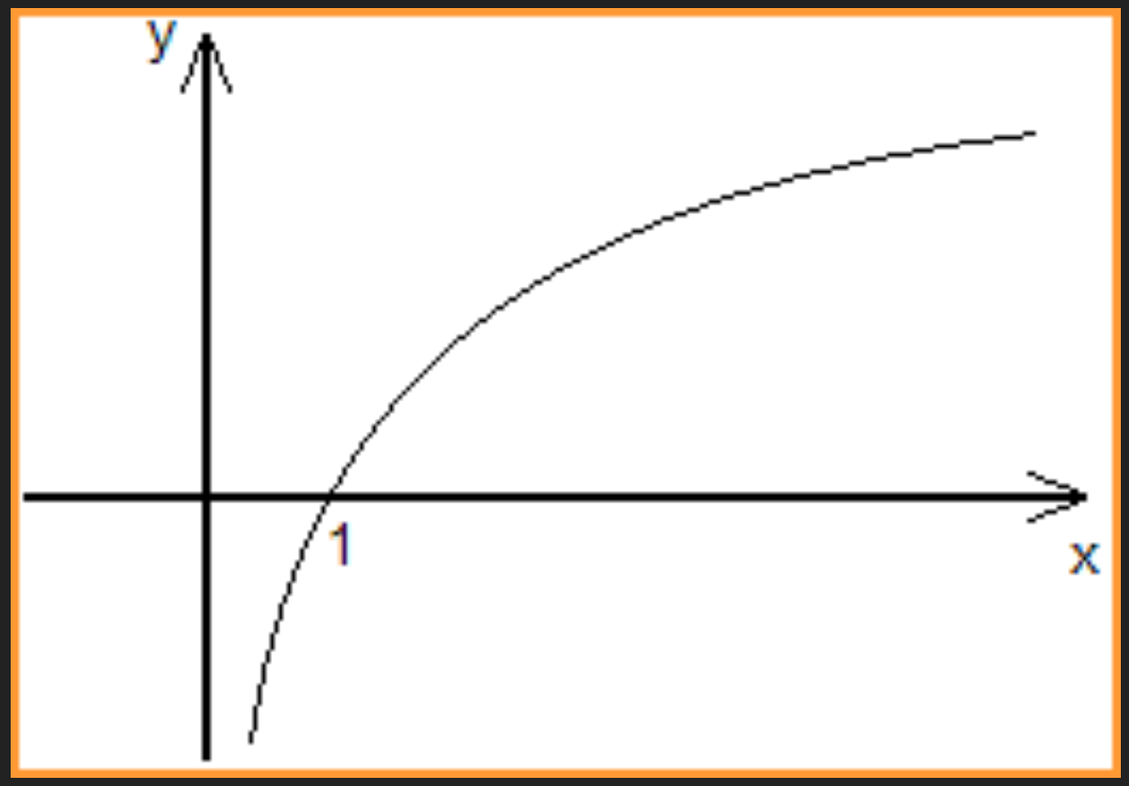
- Noção de logaritmo
- Noção de logaritmo discreto
- Logaritmo discreto
- Sistemas criptográficos que ocorrem a logaritmos discretos
- Complexidade
- Algoritmos de Colisão

NOÇÃO DE LOGARITMO

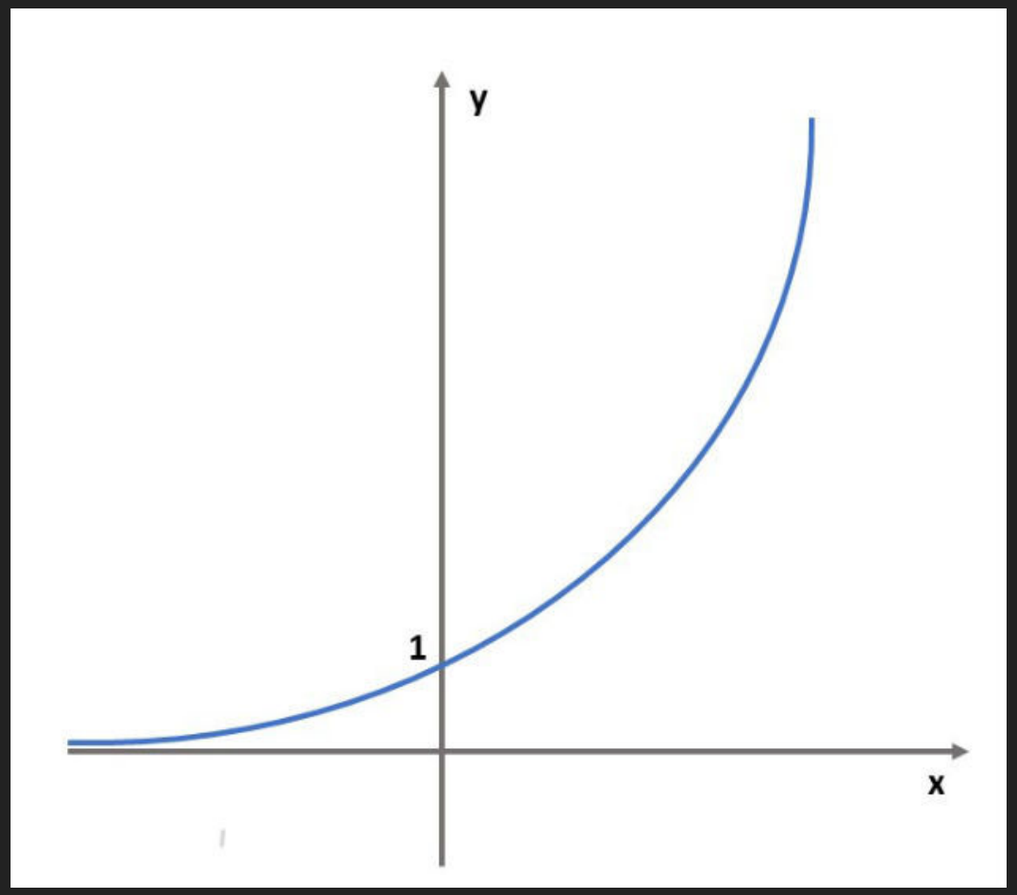
- Um logaritmo de um numero é o valor ao qual outro valor fixo deve ser elevado de forma a obteremos o valor original

$$g^x = h \quad <=> \quad x = \log_g(h)$$

GRÁFICOS



h =log2(x)



h = 2^x

LOGARITMO DISCRETO

NOÇÃO DE LOGARITMO DISCRETO

$$g^x \equiv h \pmod{p}$$

Pretendemos saber quais são os valores que *x* pode tomar, para que o resto da divisão inteira entre *g^x* e *p* dê o valor de *h*.

p tem e ser um primo.

- Exemplo:

$$2^x mod 7 = 4$$
$$x = 2 \text{ ou } x = 5$$
$$x = \{1, \ldots, 6\}$$

- Se pegarmos no 2 e no 5 vemos que são possiveis soluções para a equação de cima:

$$2^2 mod 7 = 4 \text{ e } 2^5 mod 7 = 4$$

RAÍZ PRIMITIVA

Exemplo $g^x mod 7 = resto$ x = {1,…,6} modulo p = 7

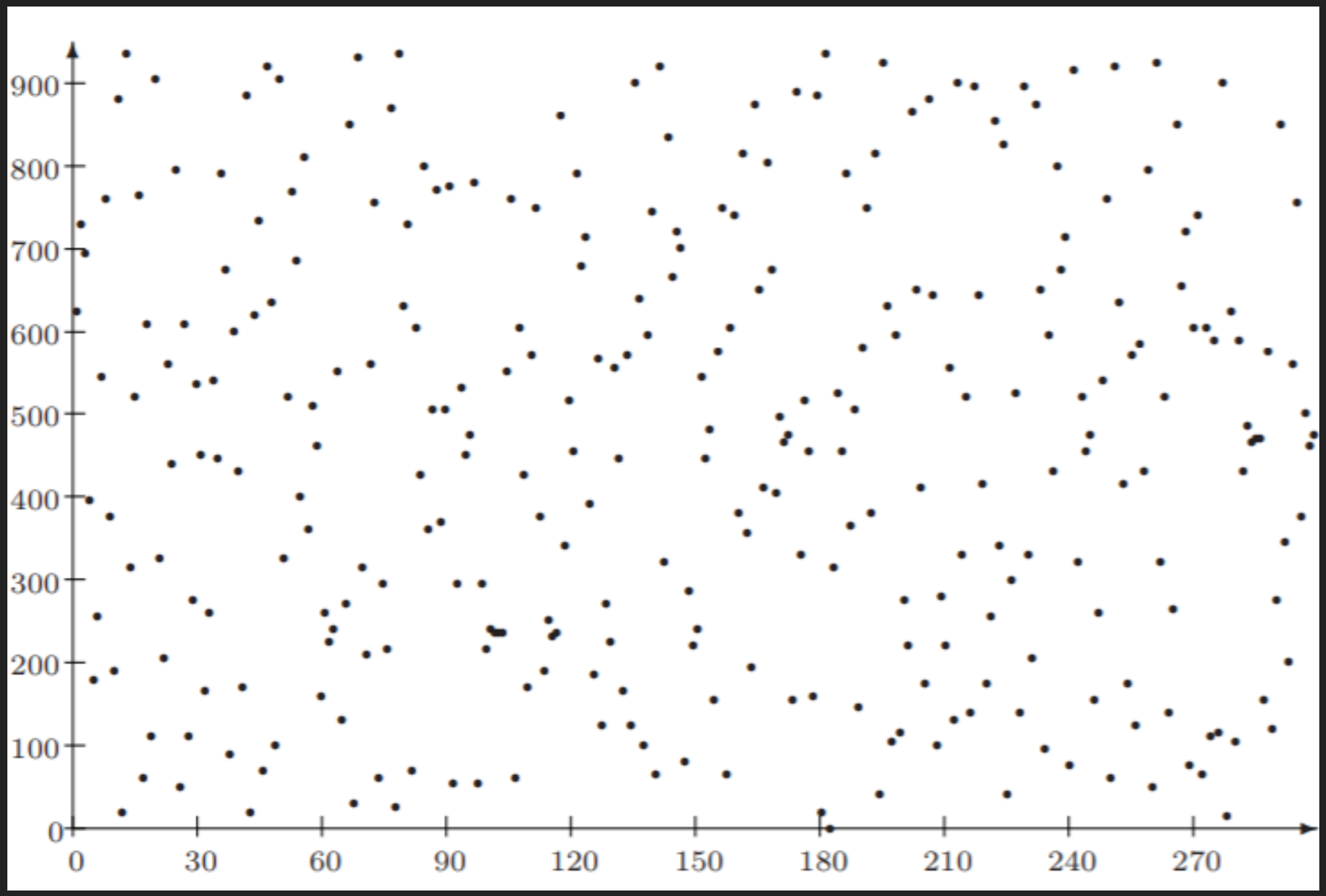
b	$b^1 mod 7$	$b^2 mod 7$	$b^3 mod 7$	$b^4 mod 7$	$b^5 mod 7$	$b^6 mod 7$
1	1	1	1	1	1	1
2	2	4	1	2	4	1
3	**3**	**2**	**6**	**4**	**5**	**1**
4	4	2	1	4	2	1
5	**5**	**4**	**6**	**2**	**3**	**1**
6	6	1	6	1	1	1

Aqui vemos que se usarmos o g=3 e g=5 conseguimos obter todos os números de 1 a 6.

RAÍZ PRIMITIVA

- Aos *g* que são elevados todos os números compreendidos de {1,.....,p-1} que conseguem gerar o grupo de valores discretos todos diferentes que possuí o mesmo intervalo mencionado anteriormente chamam-se *raízes primitivas* ou *geradores*. Ao grupo que eles geram identificamos por Z*p, onde o asterisco significa que o zero não consta neste grupo.
- A este grupo também chamamos de *cíclico* pois é um grupo que se vai repetir se continuasse-mos a elevar *g* a *p*, *p+1*, *p+2*, etc

GRÁFICO DE UM DLP



Sendo:

Gerador = 627

p = 941

627^x = h mod 941

SISTEMAS CRIPTOGRÁFICOS QUE RECORREM A LOGARITMOS DISCRETOS

- Diffie-Helman
- Massey-Omura
- ELGamal

CALCULO DE LOGARITMOS DISCRETOS

BIG O

- Notação que representa o tempo máximo de execução de uma operações sobre conjunto
- Limite baseado no numero de elementos do conjunto
- No caso de $\mathcal{O}(n)$ estamos a assumir que o algoritmo é calculado em n passos

CALCULO DO INVERSO MODULAR

$$g^{-1} \mod N$$

- Acha o valor de e de forma a que:

$$g * (g^{-1}) = 1 \mod N$$

$$g^{-1k} \mod N$$

$$(g^{-1})^{k} \mod N$$

TRIVIAL BOUND FOR DLP

CALCULO DE LOGARITMOS DISCRETOS

- Listar todas as n potências de base b possíveis
- Calcular todas as possibilidades de b^n e localizar na tabela o valor do logaritmo discreto
- Complexidade $\mathcal{O}(n)$

ALGORITMOS DE COLISÃO

ALGORITMOS DE COLISÃO

- Meet-in-the-middle
  - Criar duas listas
  - Localizar os elementos em comum
- Diminui a complexidade de $\mathcal{O}(n)$ para $\mathcal{O}(\sqrt{n})$

SHANKS

BABY STEP/GIANT STEP

Gonçalo Feliciano - 44292 | Joao Sampaio - 45749 - MIEI

SHANKS – BABY STEP/GIANT STEP

$$g^x \equiv h \mod N$$

- Assumindo que $g^x \equiv b \mod N$
- Selecionar uma constante k
- O valor de k deve ser $\lfloor\sqrt{odrer\ g}\rfloor + 1$
- Calcular (Lista 1) $g^1, g^2, g^3, \ldots, g^{k-1}$
- Calcular (Lista 2) $hg^{-k}, hg^{-2k}, hg^{-3k}, \ldots, hg^{-k^2}$
- O valor de hg^{-rk} e g^{k-i} deve ser calculado em $\mod N$

SHANKS – BABY STEP/GIANT STEP

$$g^x \equiv h \mod N$$

- Assumindo que os valores em comum são g^n e hg^{-mk}
- Podemos afirmar que:

$$g^n \equiv hg^{-mk} \mod N$$

$$g^{n+mk} \equiv h \mod N$$

SHANKS – BABY STEP/GIANT STEP

- Para o algoritmo funcionar temos de garantir que existe pelo menos um elemento em comum entre a lista 1 e lista 2

- $x = nq + r$

COMPLEXIDADE

- Assumindo o problema $g^x \equiv h \mod N$
- Se G for um conjunto
- $a \in G$
- Sendo a um elemento de ordem $N \geq 2$
- O logaritmo discreto e resolvido em $\mathcal{O}(\sqrt{N} . \log N)$ passos

ALGORITMO / ANALISE DE COMPLEXIDADE

- Assumindo que o primeiro calculo é $u = a^{-n}$
- Criamos a Lista 2 calculando $h, h * u, h * u^2, \ldots, h * u^n$
- Criamos a Lista 1 calculado $g, g^2, \ldots, g^{k-1}$
- O cálculos das listas ocorre em $\mathcal{O}(2n) \iff \mathcal{O}(n)$
- É possível encontrar os valores iguais em $\mathcal{O}(\log n)$
- Com base nisto podemos assumir que a complexidade e:

$$\mathcal{O}(n \log n) \iff \mathcal{O}(\sqrt{N} \,.\, \log N)$$

BABY STEP/GIANT STEP – EXEMPLO

$3^x \equiv 19 \mod 59$

- Assumindo $k = 5$ $N = 59$
  $g = 3$
  $h = 19$

K	$g^1, g^2, g^3, \ldots, g^{k-1} \mod N$	$hg^{-k}, hg^{-2k}, \ldots, hg^{-rk} \mod N$	g^{-rk}
1	$3^1 \equiv 3$	$19 * (3^{-5}) \equiv 28$	$3^{-1} \equiv 20$
2	$3^2 \equiv 9$	$19 * (3^{-10}) \equiv 4$	$3^{-5} \equiv 17$
3	$3^3 \equiv 27$	$19 * (3^{-15}) \equiv 9$	$3^{-10} \equiv 53$
4	$3^4 \equiv 22$		$3^{-15} \equiv 16$
5			

BABY STEP/GIANT STEP – EXEMPLO

$3^x \equiv 19 \mod 59$

- Assumindo $k = 5$ $N = 59$
  $g = 3$
  $h = 19$

K	$g^1, g^2, g^3, \ldots, g^{k-1} \mod N$	$hg^{-k}, hg^{-2k}, \ldots, hg^{-rk} \mod N$	g^{-rk}
1			
2	$3^2 \equiv 9$		
3		$19 * (3^{-15}) \equiv 9$	
4			
5			

BABY STEP/GIANT STEP - EXEMPLO

$3^x \equiv 19 \mod 59$

$k = 5 \qquad N = 59$
$g = 3$
$h = 19$

$3^2 \equiv 9 \qquad 19 * (3^{-15}) \equiv 9$

$19 * (3^{-15}) \equiv 3^2 \iff 3^{15+2} \equiv 19 \mod 59$

$3^{17} \equiv 19 \mod 59$

SHANKS - BABY STEP/GIANT STEP - EXEMPLO

$$g^x \equiv h \mod N$$

$$9704^x \equiv 13896 \mod 17389$$

- Assumindo $k = \lfloor \sqrt{1242} \rfloor + 1 = 36 \quad N = 17389$

$$g = 9704$$

$$h = 13896$$

k	g^k	$h \cdot u^k$	k	g^k	$h \cdot u^k$	k	g^k	$h \cdot u^k$	k	g^k	$h \cdot u^k$
1	9704	347	9	15774	16564	17	10137	10230	25	4970	12260
2	6181	13357	10	12918	11741	18	17264	3957	26	9183	6578
3	5763	12423	11	16360	16367	19	4230	9195	27	10596	7705
4	1128	13153	12	13259	7315	20	9880	13628	28	2427	1425
5	8431	7928	13	4125	2549	21	9963	10126	29	6902	6594
6	16568	1139	14	16911	10221	22	15501	5416	30	11969	12831
7	**14567**	6259	15	4351	16289	23	6854	13640	31	6045	4754
8	2987	12013	16	1612	4062	24	15680	5276	32	7583	**14567**

$$u = g^{-n} \iff 9704^{-36} = 2494$$

SHANKS - BABY STEP/GIANT STEP - EXEMPLO

$g^x \equiv h \mod N$

$9704^7 = 14567 \mod 17389$

$13896 * 2494^{32} = 14567 \mod 17389$

$9704^7 = 13896 * 2494^{32} \mod 17389$

$9704^x \equiv 13896 \mod 17389$

$a^n \equiv ba^{-mk} \mod N$

$a^{n+mk} \equiv b \mod N$

$k = 36$

$g = 9704$

$h = 13896$

$N = 17389$

SHANKS - BABY STEP/GIANT STEP - EXEMPLO

$$g^x \equiv h \mod N$$

$$9704^7 = 14567 \mod 17389$$

$$13896 * 2494^{32} = 14567 \mod 17389$$

$$9704^x \equiv 13896 \mod 17389$$

$$a^n \equiv ba^{-mk} \mod N$$

$$a^{n+mk} \equiv b \mod N$$

$$k = 36$$

$$g = 9704$$

$$h = 13896$$

$$N = 17389$$

$$9704^{-36} = 2494$$

$$13896 = 9707^7 * 2494^{-32} \iff 9704^7 * (9704^{36})^{32}$$

$$9704^{1159}$$

$$9704^{1159} \equiv 13896 \mod 17389$$

BIBLIOGRAFIA

- Hoffstein, Jeffrey, Pipher, Jill e Silverman, J.H. . (2008). An Introduction to Mathematical Cryptography. Springer
- Cruise, Brit. O problema do logarítmo discreto. Acedido em: 30, maio, 2019, em: https://pt.khanacademy.org/computing/computer-science/cryptography/modern-crypt/v/discrete-logarithm-problem.
- Cormen,Thomas, Balkcom, Devin, Khan Academy. Notação Big-O. Acedido em: 30, maio, 2019, em: https://pt.khanacademy.org/computing/computer-science/algorithms/asymptotic-notation/a/big-o-notation
- Khan Academy. Modular inverses. Acedido em: 3, Abril, 2019, em: https://www.khanacademy.org/computing/computer-science/cryptography/modarithmetic/a/modular-inverses
- https://www.youtube.com/watch?v=57SUNQL4JFA
- https://www.youtube.com/watch?v=007MVsELvQw
- https://www.youtube.com/watch?v=FvInAqxzjsM
- https://www.youtube.com/watch?v=BRMj5jE6Z-U

BIBLIOGRAFIA

- https://www.youtube.com/watch?v=EOcQshMv8UA
- https://www.youtube.com/watch?v=GSIDS_lvRv4