FRS- Universidade Federal do Rio de S	Suneivo ad a come la ballata *a
io de Saneiro, 08 de Sunho de 201º	
a sologial of malling can	returne in a constant (all me)
PROBLEMA: DO LOGARITMO DISCRETO:	who and combe not more about and and
- caso Gerac: dado um grupo gx = h em G.	(6, x), eg, h & G, determinar X tal que
- CASO PARTICULAR EM U(n)	dados y, h & U(n), determinar x tal que
gx = h (mod n)	9-1-9-2009742
	solução, isto é, tal x nem sempre existe. Entre-
	is for um gerador do grupo, então o problema
sempre tem solução, já que, com	o g é gerador, todo elemento h do grupo pode
ser eserito como potência de g.	3 = 4 1
450	Agriculate to alconocia is
No caso do El Gamal, uti	I zamos o grupo U(p), com p primo (que é ciclico,
pelo teorema da vais primitival e	um gerador g de Ucpi. A chave privada é um in-
	1=axp-1 a chave publica c é on forma reducida
de ga modulo p.	was properly and a second of the second
- Valores publicus: 9, p,c	
· Valor parado. a	The state of the s
Esses quatro valores satizfaz	eem a relação
Bo = c (wod b)	Comment on 1988: The D. Paper 1988 America of Co.
	a partir dos valores públicos, preciso resolver o
seguinte problema do logaritmo	
· (Macx mic	March fall of material M. 1987.
	tilibr

gx = h (mod p) -> 0 < x < p-1	The first state of the
Como U(p) é cíclico e g é um gerador, e logaritmo discreto sampre tem solução. Essa solução	esse problems d. 1.
- ALGORITMOS PARA A RESOLUÇÃO DO PROBLEMA DO CO	
1) ALGORITMO INGÉNUO:	3 ms d = x
my bet & you do to find 3 or ye work to	V SA MARKETON - CONTRACTOR
ENTRADA: 81416	(-lam) d=xa
saipa: x tal que gx = h (mod p)	I agree of the transport
solding a city of the plant of a	7344
Instruções:	a property invites out you
4) X 4-0	y bushing the
2) Enquanto g" # h (mod p),	faça:
2.1) X < x + 1	e leage II st som I
3) Retorne a	a fee doo a sure to your of
and the same problem of the same	-late to an always are a second
Este algoritmo é eficiente se p for pegrens.	7 1 2 2
Logo, uma condigão necessária (mas que no	io o supiciente soziahal sova a
wroned do El Engl	a sharp all
L> RECOMENDAGÃO ATUAL: P com 512 bits ou p	com 1024 bits
2) ALCORITHO BABY-STEP GIBNT-STEP DE SHANKS	(+ L -) > = 20
Vamos descrevê-la para um grupo U(n):	2 704/6 my 22 12/13
at a constant	a miles of the secondaries which
libra Seja K a orden de U(n) (se n for	Primo K= N~1).

· / - 1	
. Calculamos m=[VK]+1 (no caso de Ucp), m=[10-1-1-1
Seja x ol solução do problema do logaritmo discret	o ide make and a market
gx = h (mod n)	7 6 K 2K
u eserever x como:	mr i ge
x=i m +j,	(06m) n2 *2
om O≤i,j <m< td=""><td>(n band (= 1 ** ** **)</td></m<>	(n band (= 1 ** ** **)
Se i for o quiciente de x for m ej for o como jé o resto de uma divisão por m, então.	resto de x por m, então i e j co
o < j < m	-0.473 (-1804 (3-pays (1)
ramos supor que i também está nesse intervalo.	or sis O so sol
Suponha, por contradições que ism.	1-stani g
END X >> m + 5 = m2+j = ([1] +1)2+j >	9 9
DESERVISÃO: [VR] = VK = [VR]+1	
Temos então	
x>K	11-con 2 = g -1-103-11

Entretanto, isso não é possível. Como x é a ordem do grupo, o expoente x deve estar no intervalo OEX EX Logo, ism. gx = h (mod n) q'm+j = h (mod n) gim. gizh (mod n)

gi = h. (g-1) im (mod n)

- CALCULO OS BABY - STEPS !

Para j de O até m-1, calculo a forma reduzida de gi módulo n e guardo isso numa tabela:

j	g ⁱ smoot n)
0	4
9	5
m -4	(ntoms) mg

- CALCULO OS GIANT - STEPS

1) calulo g'= g (moda) (usando o extidiano estendido)

z) Calculo t = (g') [mod n)

ico se	Para cada i de C esse valor a parece i. Se aparece, t	na tabela	dos bab	y-sles	5, 5	e não	aparee	e vou po	Na c
								9	
				- 63	5	1	23	,	
7:427								1	
)=3									
								pa	
Vamos re	solver o problema de	logaritmo disc	reto:	J1)/H	0		AP.	2.9	
3,	= 2 (mod 127)							TP : 1	
יחב [אף-1	+4 = [-126] +1 =	1171=12			77.	19	37_3	- لم دهد	
Baby-Steps		. Ĝl	9NT-STEPS		or ou	. 1	1	3.	
j	3 mod 127	1) CALC	1) CAZCULO O INVERSO DE 9:						
0	1				J	7.5		Ā	
4	3	R	Q.	×	У	ut		E	
2	9	3	-	1	ь	. , þ		ř	
3	27	127	_	O	4	F		7	
4	81	9	0	1	O	1		3	
5	116	1	42	-42	4				7
6	94	0	8		-			1-1	
7	28							0-6	
g	84	-42 = 8	5 (mod	127)					
9	125						8	tooks	De l
10	121	o' = 85					= 0	1 2 3 4	à
11	109	-							

tilibra

CONTINUAÇÃO DOS GIANT. STEPS

		2 .1m
2)	CALENTO	(a)
	17	0

	E IMDIE ?	E	A	R
	NÃO	12	85	4
C1-	Não	6	113	4
p-	514	3	69	1
	514	1	62	69
	พลัง	0	34	8 7

£= 87

- CALCULO DOS BABY-STEPS;

j.	h. t mod 127	C 4 1808		
0	2			
4	47	7	Kalibara B. L.	į
2	25			0
3	16			
4	422		F	
5	73	-	18	6
6	1	n 1 6	(1)	