Algoritmos e Criptografia

15/06/2018

Algoritmos

>>Oquê? Quando? Onde? Quem?

O que pode ser definido como um algoritmo?

Algoritmos

>>Oquê? Quando? Onde? Quem?

Conjunto de etapas para executar uma tarefa. Este conjunto de etapas precisa ter precisão suficiente para que a tarefa seja executada.

portanto....

Algoritmos

Podemos dizer que os algoritmos são universais ?

Princípio da generalidade: Executa a tarefa em qualquer input numérico enviado?

Eles podem ser caracterizados e medidos?

Algoritmos

SIM
AMIGUINHO!

Algoritmos

>>cuma??

Possuem propriedades e condições: condição na entrada (input), tempo de execução, a condição na saída e a lógica que orienta o tratamento da informação.

***AKS -> general*, *polynomial*, *deterministic*, and *unconditional*.**

Algoritmos

>>cuma??

***AKS -> general*, *polynomial*, *deterministic*, and *unconditional*.**

Algoritmos

>>cuma??

General -> Avaliação da entrada não em termos de linguagem e sim de condição numérica: para todos os números e não com específicas propriedades numéricas.

Polynomial -> Característica de tempo de crescimento e execução da sua cadeia de etapas analisada sob como ela foi escrita. -> BigO, assintótica.

D*eterministic ->* *Sua cadeia de comandos tem um resultado exato e não provável (probabilidade no result).*

Unconditional -> Quando sua exatidão não depende de uma condição lógica ou lei (por ex uma teoria não completamente provada)

Criptografia RSA

simétrica

A B C D E F G
1 2 3 4 5 6 7

Criptografia simples

_> somente por conhecer o método pode tornar a msg legível

_> depende dos dois (emissor e receptor) serem detentores do método

_> pode ser quebrada matematicamente aplicando análise de recorrência

assimétrica

CHAVE PÚBLICA
obtida pelo produto de dois valores 2048 bits, aprox 617 dígitos

Criptografia RSA

_> chave pública e chave privada

_> não depende dos dois (emissor e receptor) possuírem o método

_> difícil de ser quebrada matematicamente

Cryptografia RSA

>>primalidade

A criptografia RSA é baseada em números primos, é construída com números realmente grandes (n^x) .

Com base num valor de chave pública os métodos de criptografia realizam a FATORAÇÃO entre as chaves para descobrir seu valor único de PRIMALIDADE.

Exceção e erro: Pode ocorrer pois uma resposta de um número definitivamente não primo é absoluta e correta, pois já encontrou um FATOR que o divide mas se declarar que ele é primo, pode ser ainda que ele não é primo pois pode haver (1 em mais de 40 bilhões de ocorrências) divisor dele que não foi “descoberto” (calculado).

Cryptografia RSA

>>primalidade

Porque é difícil de ser quebrada?

PRIMALIDADE DE CHAVE PÚBLICA

chave publica = n

primo1 = p

primo2 = q

*n = p * q*

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100
101	102	103	104	105	106	107	108	109	110
111	112	113	114	115	116	117	118	119	120

Prime numbers

Como funciona

Pré codificação

Etapa de conversão da mensagem

A -> 10
z -> 35
espaço -> 99

(A..Z) = (10..35)

Totiente (co-primo) x

φ(n) = (**p** - 1) * (**q** - 1)

Quantidade de co-primos de N < N, para:

p = 17, **q** = 41

φ(697) = (**17** - 1) * (**41** - 1)

φ(697) = 640

Calculando a chave pública

MDC(640, 2) = 2 -> não representa
MDC(640, 3) = 1 -> representa

MDC(640,13) = 1 = e

Chave pública = (n, e)
Chave pública = (697, 13)

Cifrando a mensagem

Operação modular -> Se **y** divide **x**, podemos dizer que

$$x : y = c$$

portanto, existe um **c** tal que

$$x = \mathbf{c} * y + \mathbf{r}\ \textbf{(r é o resto se houver)}$$

$$23 : 7 = c$$

$$\mathbf{23} = 3 * 7 + \mathbf{2}$$

Cifrando a mensagem

$$c = \mathbf{m} \wedge \mathbf{e} \bmod \mathbf{n}$$

A mensagem cifrada é c = mensagem

onde **e** é a chave pública e **m** é o valor numérico da letra que queremos cifrar do nosso alfabeto.

Ciframos cada letra!!!

(to be continued...)