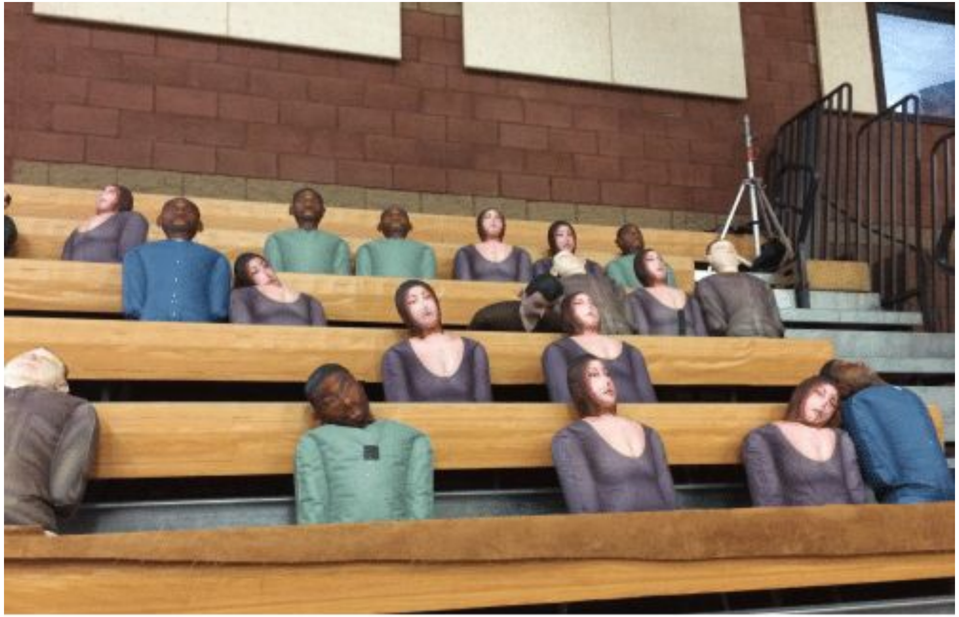
INE5429-07208
Segurança em Computação
Matemática para Criptografia e Criptografia Assimétrica

Prof. Jean Everson Martina

O que vimos na aula passada:

- Modelos de Criptografia
- Criptografia x Criptoanálise
- Incondicionalmente x Computacionalmente Seguro
- Técnicas de Substituição
- Técnicas de Transposição
- Maquinas de Rotores
- Esteganografia
- Cifradores Simétricos
- DES – Data Encryption Standard
- AES – Advanced Encryption Standard

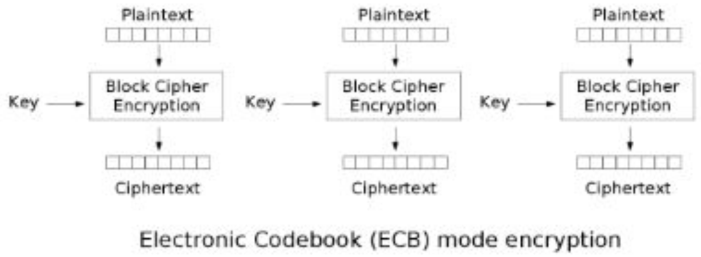


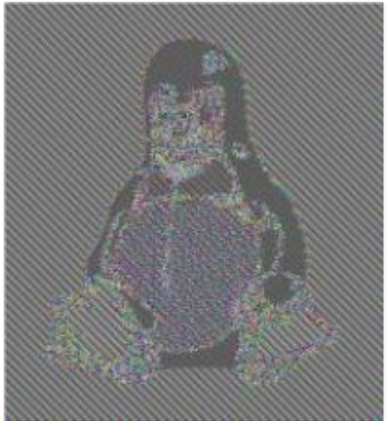
Modos de Operação

- Usar cifradores simétricos exige táticas, ou mesmo com o melhor cifrador ficamos vulneráveis!
- Modos de Operação:
  - Electronic Codebook -ECB
  - Cipher Block Chaining - CBC
  - Cipher Feedback - CFB
  - Output Feedback - OFB
  - Counter Mode - CTR

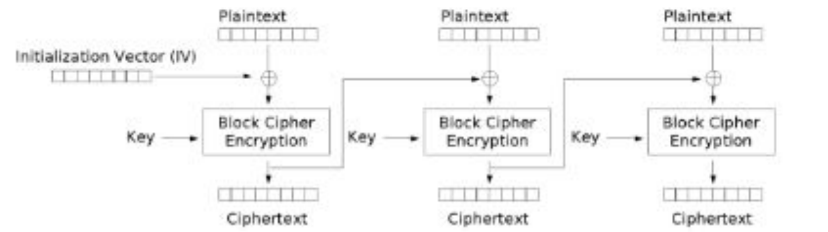
ECB

- Cada bloco é codificado de forma independente
- Segurança para transmissão de dados únicos

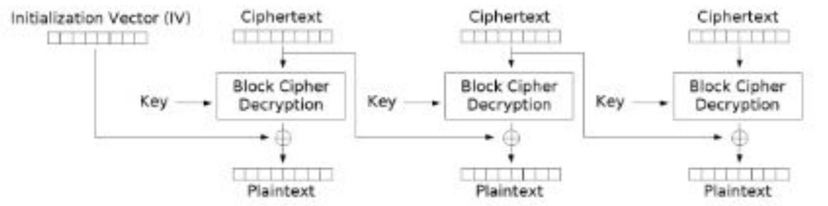




CBC



Cipher Block Chaining (CBC) mode encryption

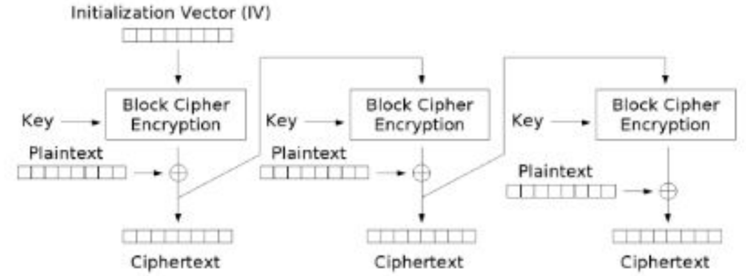


Cipher Block Chaining (CBC) mode decryption

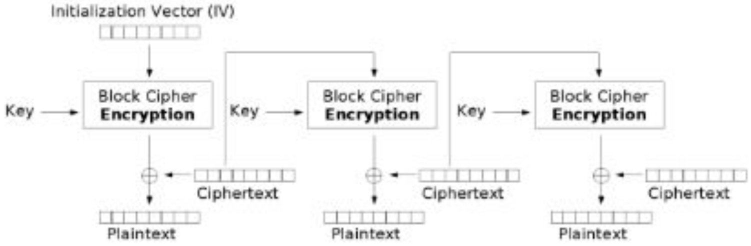
- A entrada é XOR do próximo bloco de texto claro e o bloco anterior cifrado
- Uso para transmissão de dados e autenticação

CFB

- O texto cifrado é XOR com o texto claro e retroalimentado no cifrador
- Uso para transmissão de dados e autenticação

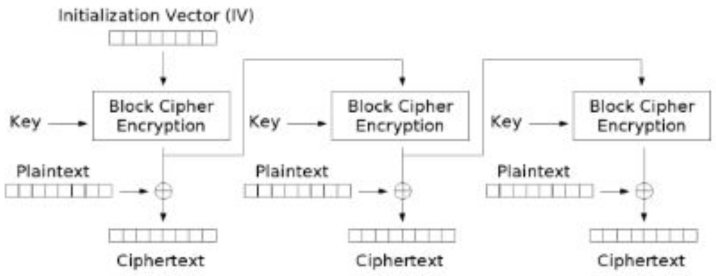


Cipher Feedback (CFB) mode encryption

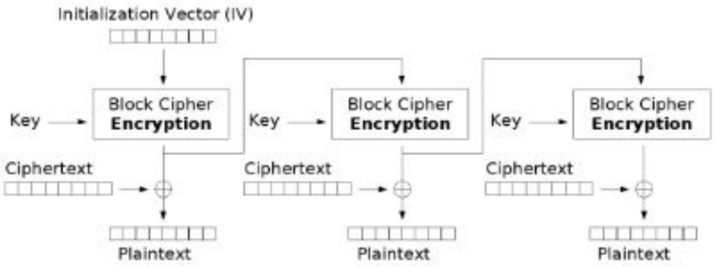


Cipher Feedback (CFB) mode decryption

OFB



Output Feedback (OFB) mode encryption

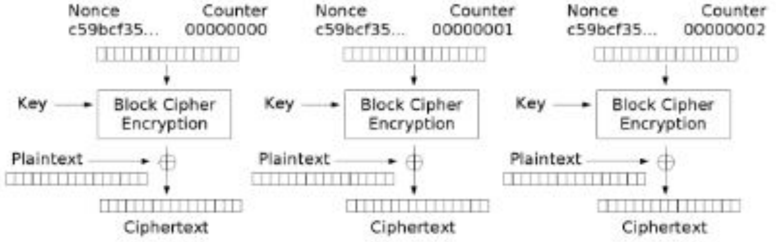


Output Feedback (OFB) mode decryption

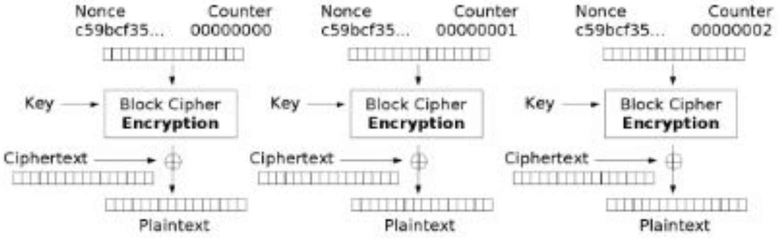
- Similar a CFB. A saída do cifrador é retroalimentada para gerar um stream de bits
- Usado em canais ruidosos

CTR

- Cada bloco é XORed com um contador cifrado
- Uso geral em transmissão de dados e em links de alta velocidade

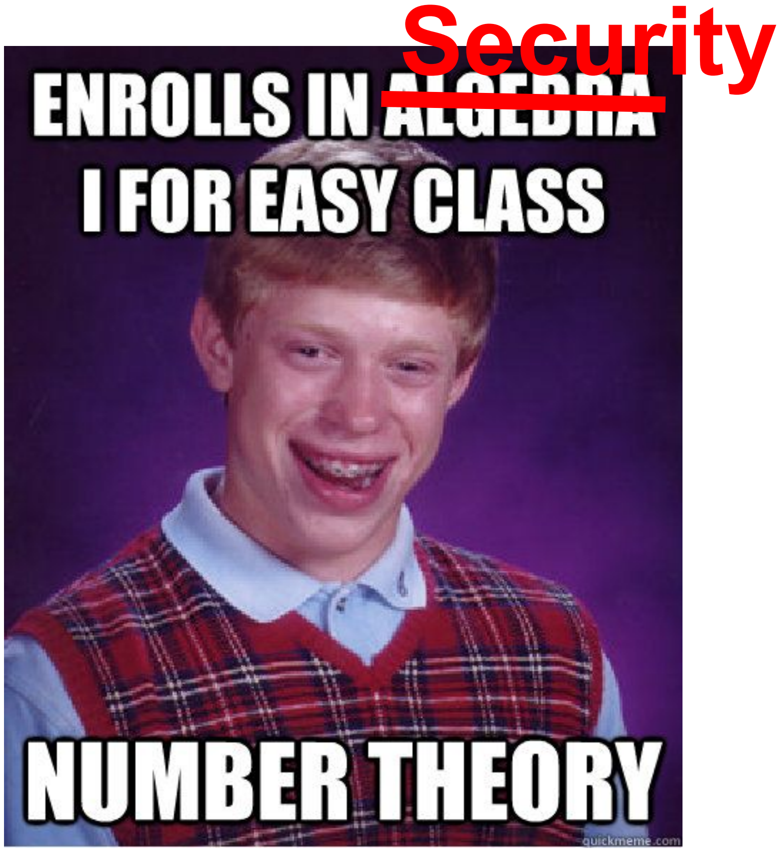


Counter (CTR) mode encryption



Counter (CTR) mode decryption

Teoria de Números



- Números Primos
- Teoremas de Euler e Fermat
- Teste de Primalidade
- Teorema Chinês do Resto
- Logaritmo Discreto.

Números Primos

- Primo é um inteiro que só pode ser dividido por 1 e por ele mesmo sem resto
- Todo número inteiro pode ser representado por uma fatoração de primos
- 12 = a2=2, a3=1, 91 = a7=1,a13=1
- Multiplicação de números inteiros pode ser feita pela adição de fatores primos
- Nós podemos saber que um número divide outro se o expoente do primeiro primo do divisor é ≤ que o do dividendo
- Calcular o MDC de números expressos em notação prima é a multiplicação dos primos pelo menor expoente
- Isso só funciona facilmente para não primos

Table 8.1 Primes under 2000

2	101	211	307	401	503	601	701	809	0	1009	1103	1201	1301	1409	1511	1601	1709	1801	1901
3	103	223	311	409	509	607	709	811	911	1013	1109	1213	1303	1423	1523	1607	1721	1811	1907
5	107	227	313	419	521	613	719	821	919	1019	1117	1217	1307	1427	1531	1609	1723	1823	1913
7	109	229	317	421	523	617	727	823	929	1021	1123	1223	1319	1429	1543	1613	1733	1831	1931
11	113	233	331	431	541	619	733	827	937	1031	1129	1229	1321	1433	1549	1619	1741	1847	1933
13	127	239	337	433	547	631	739	829	941	1033	1151	1231	1327	1439	1553	1621	1747	1861	1949
17	131	241	347	439	557	641	743	839	947	1039	1153	1237	1361	1447	1559	1627	1753	1867	1951
19	137	251	349	443	563	643	751	853	953	1049	1163	1249	1367	1451	1567	1637	1759	1871	1973
23	139	257	353	449	569	647	757	857	967	1051	1171	1259	1373	1453	1571	1657	1777	1873	1979
29	149	263	359	457	571	653	761	859	971	1061	1181	1277	1381	1459	1579	1663	1783	1877	1987
31	151	269	367	461	577	659	769	863	977	1063	1187	1279	1399	1471	1583	1667	1787	1879	1999
37	157	271	373	463	587	661	773	877	983	1069	1193	1283		1481	1597	1669	1789	1889	1997
41	163	277	379	467	593	673	787	881	991	1087		1289		1483		1693			1999
43	167	281	383	479	599	677	797	883	997	1091		1291		1487		1697			
47	173	283	389	487		683		887		1093		1297		1489		1699			
53	179	293	397	491		691				1097				1493					
59	181			499										1499					
61	191																		
67	193																		
71	197																		
73	199																		
79																			
83																			
89																			
97																			

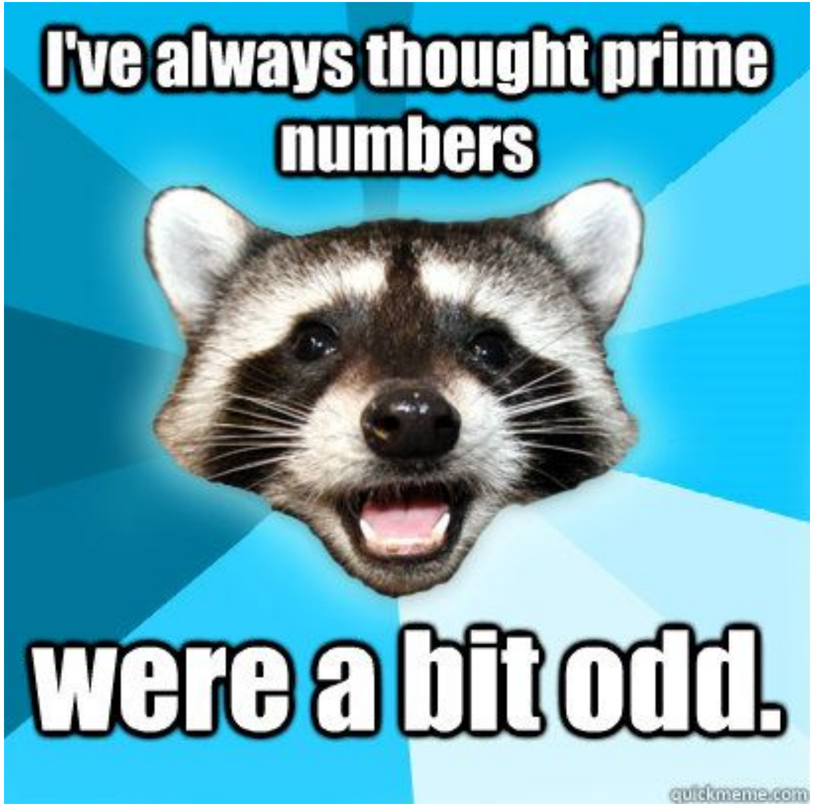
Teorema de Fermat

- Se p é primo e a é um inteiro positivo não divisível por p então $ap-1 \equiv 1(\text{mod } p)$
- Forma alternativa: $ap \equiv a(\text{mod } p)$
- Requer que p e a sejam relativamente primos
- $p=5, a=3 \rightarrow ap=35=243 \equiv 3(\text{mod } 5)=a(\text{mod } p)$

Função Totiente e Teorema de Euler

- A função é escrita ϕ(n) e é definida como a quantidade de números relativamente primos a n menor que n
- Φ(1) = 1, Φ(35) = 24 → {1,2,3,4,6,8,9,11,12,13,16,17,18,19,22,23, 24,26,27,29,31,32,33,34}
- ϕ(p) = p – 1
- ϕ(n) = ϕ(pq) = ϕ(p)x ϕ(q)= (p-1) (q-1)
- Teorema:
  - Para todo a e n que são relativamente primos aϕ(n) ≡ 1 (mod n)
  - a = 3, n = 10, ϕ(10) = 4
  - aϕ(n) = 34 = 81 ≡ 1 (mod 10) = 1 (mod n)
  - Versão alternativa:
  - aϕ(n)+1 ≡ a (mod n)

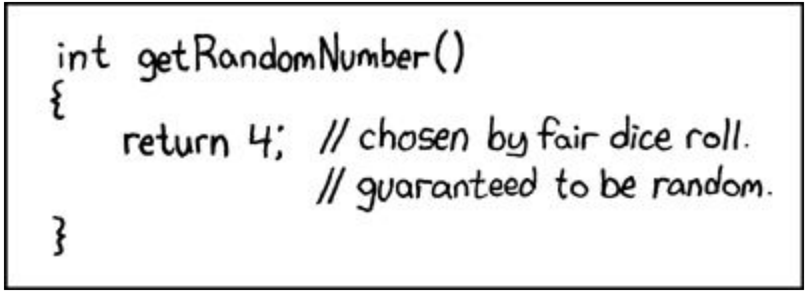
Teste de Primalidade



- Saber se um número é primo é importante para afirmar o teorema de Fermat
- Temos que trabalhar com números das ordem de grandeza de 1024 bits
- Algoritmo de Miller-Rabin
    - Test(n) – n impar
    - 1. ache k, q inteiros k > 0, q impar | (n-1=2kq)
    - 2. rand(int a) → 1 < a < n-1
    - 3. Se aq mod n = 1 → Inconclusivo
    - 4. para j = 0 ate k -1 faca
    - 5. se a2jq mod n ≡ n – 1 → Inconclusivo
    - 6. Composto

Geradores de Números Aleatórios

- Uso:
  - Geração de chaves
  - Geração de parâmetros
  - Controles de sessão
- Aleatoriedade:
  - Distribuição uniforme → fácil
  - Independência → difícil
- Estratégia similar a Miller-Rabin
- Não previsibilidade → nonces
- Solução determinística x não determinística
- Geradores Pseudo-Aleatórios:
  - Deterministico
  - Passa testes de aleatoriedade
  - Aleatoriedade relativa
- Geradores de Congruência Linear
- Geradores Criptográficos

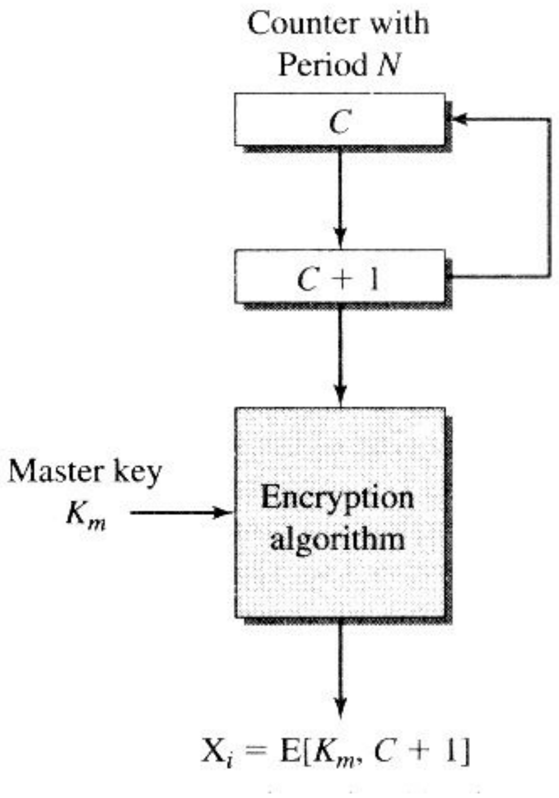


Geradores de Congruência Linear

- Modulo m, multiplicador a, incremento c e semente inicial X0
- $Xn+1 = (aXn+ c) \bmod m$, $0 \leq Xn < m$
- Dependente na boa escolha de parâmetros
- M perto ou igual a 231
  - Um bom a é difícil → um punhado em 2 bilhões pra ter um período próximo a m
  - normalmente a = 16807

Geradores Criptográficos

- Cifragem cíclica
- Bom para chaves de sessão
- DES em OFB com a semente sendo a chave
- ANSI X9.17: 3 triple-DES é um dos mais robustos



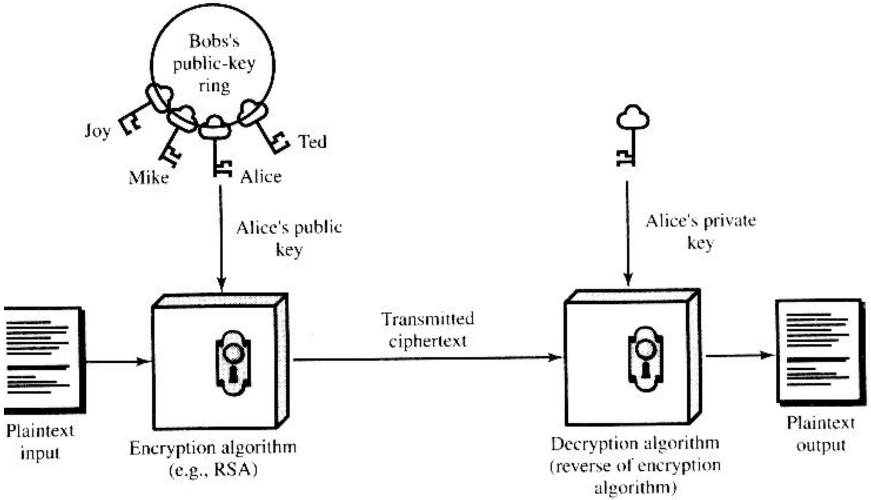
Logaritmo Discreto

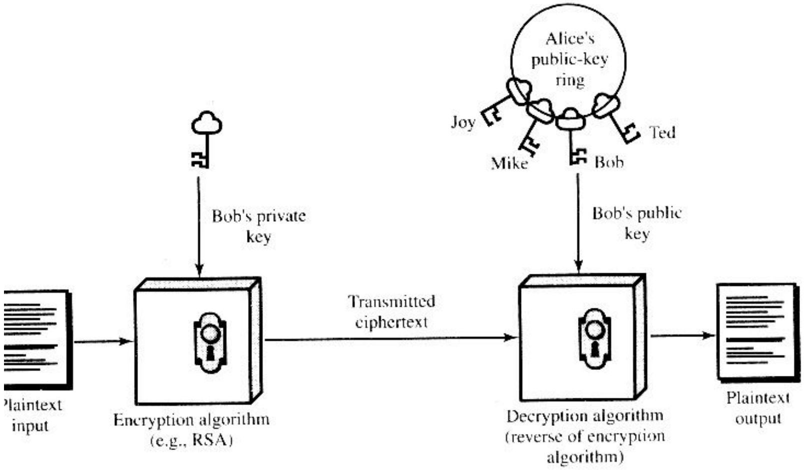
- Diffie-Hellman e DSA
- loga(b)=x → ax =b
- É o logaritmos calculado Zp
- 34 mod 17 = 13 → 3k = 13 (mod 17)
  - 4 é uma solução, mas na verdade inúmeras soluções existem→ 4 + 16n =log3(13 mod 17)
  - Equivalente a k = 4 mod 16
- Não existe algoritmo eficiente para isso
- Força bruta: elevar a base a maiores potência de k ate achar o g certo
- Funciona para criptografia, porque é fácil fazer com a exponenciação
- Assimetria equivalente da multiplicação e fatoração de números primos
- Eficiente em outros grupos (curvas elípticas)

Princípios de Criptossistemas de Chave Pública

- Uma chave pública e uma privada
- O que é feito com uma chave poder ser “desfeito” com outra
- Chave assimétrica prove:
  - Confidencialidade, Autenticação, e derivados
- Foi criada para responder ao problema de distribuição de chaves
- Provê assinatura digital
- É computacional impossível determinar a chave privada através da chave pública

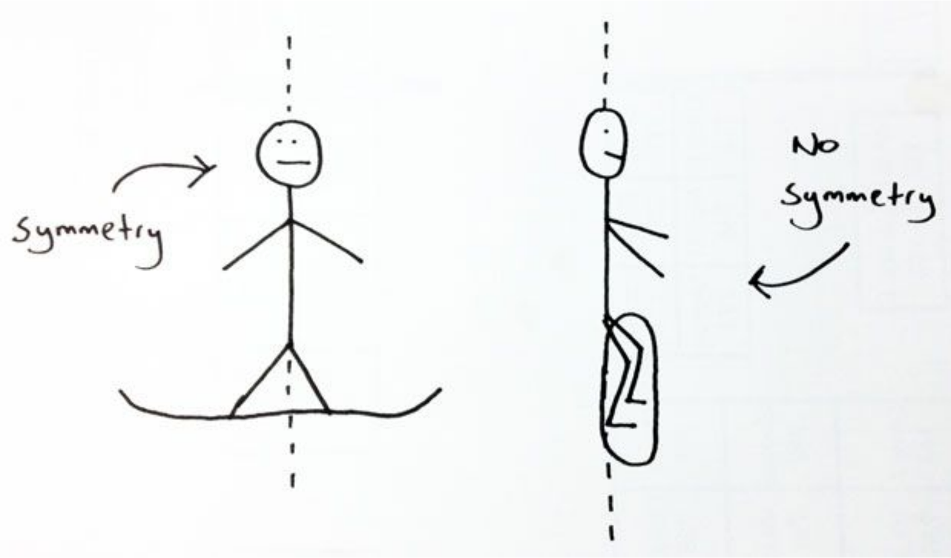
Criptossistemas de Chave Pública





(b) Authentication

Chave simétrica x Chave pública



- Chave Secreta:
  - Funcionamento:
    - Mesmo algoritmo
    - Mesma chave
  - Segurança:
    - Chave secreta
    - Impossível quebrar sem a chave
- Chave Pública:
  - Funcionamento:
    - Diferentes algoritmos
    - Pares de chaves
  - Segurança:
    - Uma chave secreta
    - Impossível derivar a outra chave
    - Impossível quebrar com uma só chave

Requisitos de Chave Pública

- Fácil (computacionalmente) gerar um par (de chaves)
- Fácil para o remetente operar com a chave pública
- Fácil para o destinatário operar com a chave privada
- Impossível determinar Kr a partir de Ku
- Impossível recuperar M conhecendo Ku e C

RSA

- 1977, Rivest, Shamir e Adelman / MIT
- É o algoritmo mais aceito
  - Base para a Web
  - Base para assinatura digital no Brasil
- Texto claro e texto cifrado são inteiros mod n
- n é normalmente 1024 bits (309 dígitos)
- É baseado em exponenciação mod p
- Algoritimo:
  - Blocos do tamanho de n
  - C = M^e mod n
  - M = Cd^ mod n = ((M^e)^d) mod n = M^e^d mod n
  - Todos conhecem n, o remetente conhece e, o destinatário conhece d
  - Chave Pública → (n, e)
  - Chave Privada → (n, d)

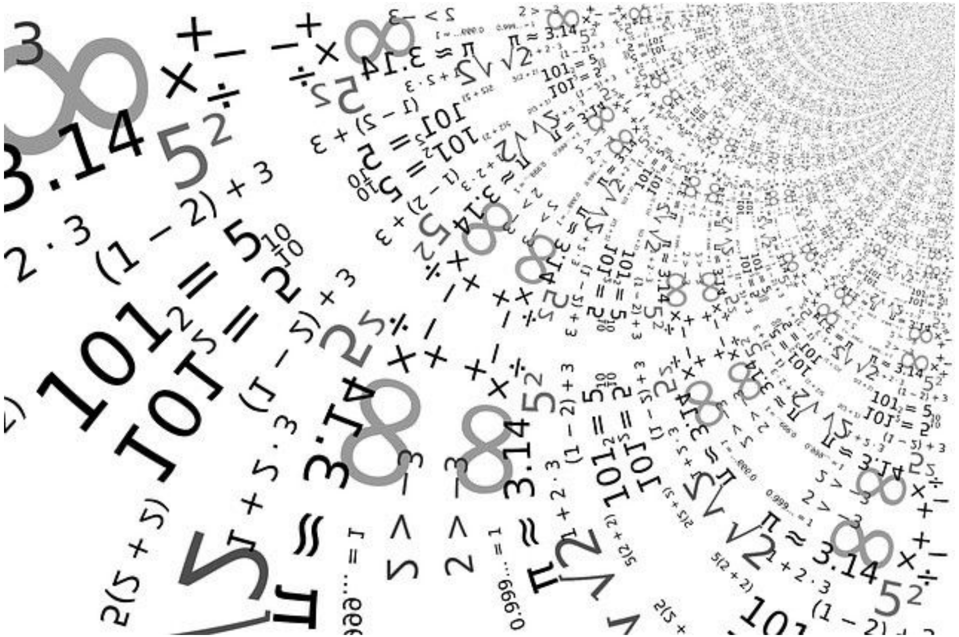
RSA - Requisitos

- e, d, n são escolhidos pra satisfazer Med mod n = M para todo M < n
- Para isso “e” e “d” devem ser multiplicativas inversas mod ϕ(n) → e.d mod ϕ(n) = 1
  - e.d ≡ 1 mod ϕ(n) → d ≡ e-1 mod ϕ(n)
  - gcd(ϕ(n),d)=1 e gcd(ϕ(n),e)=1
- p, q primos: privados e escolhidos
- n = p.q: publico e calculado
- e | gcd(ϕ(n),e) = 1 ˆ 1 < e < ϕ(n): publico e calculado
- d ≡ e-1(mod ϕ(n))
- Chave pública (e, n)
- Chave privada (d, n)

RSA na Prática

- Geração de Chaves
  - p = 17 e q = 11
  - n = porque = 17 x 11 = 187
  - $\phi(n) = (p – 1)(q – 1) = 16 \times 10 = 160$
  - e = 7, gcd(160, 7) = 1 ˆ 1 < 7 < 160
  - d | de ≡ 1(mod 160) ˆ d < 160 → d = 23
  - 23 x 7 = 161
  - Ku = {7, 187} , Kr = {23, 187}
- Cifragem
  - Texto Claro = 88
  - 887 mod 187 = 11
  - Texto cifrado = 11
  - 1123 mod 187 = 88
  - Computacionalmente intensivo de fazer com números grande
  - Teorema chinês do resto torna possível
  -

RSA - Considerações Computacionais



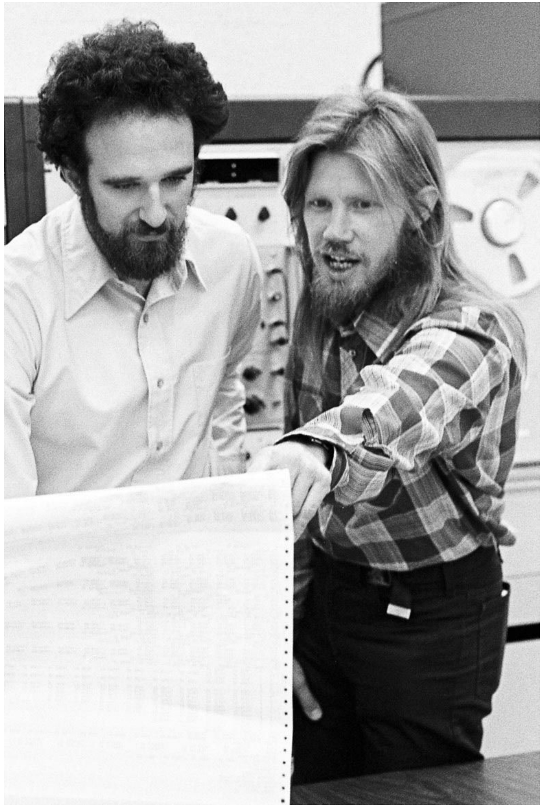
- Exponenciação mod p requer truques matemáticos
- O e acaba sendo fixo em 65537 e 17. 3 sofre ataques se utilizado muitas vezes
- d tem que ser grande para evitar força bruta
- Gerar chaves pode ser demorado pois precisamos do M-R várias vezes em um número muito grande

RSA Factoring Challenge

RSA number	Decimal digits	Binary digits	Cash prize offered	Factored on	Factored by
RSA-100	100	330	US$1,000[4]	April 1, 1991[5]	Arjen K. Lenstra
RSA-110	110	364	US$4,429[4]	April 14, 1992[5]	Arjen K. Lenstra and M.S. Manasse
RSA-120	120	397	$5,898[4]	July 9, 1993[6]	T. Denny *et al.*
RSA-129 [**]	129	426	US$100	April 26, 1994[5]	Arjen K. Lenstra *et al.*
RSA-130	130	430	US$14,527[4]	April 10, 1996	Arjen K. Lenstra *et al.*
RSA-140	140	463	US$17,226	February 2, 1999	Herman te Riele *et al.*
RSA-150	150	496		April 16, 2004	Kazumaro Aoki *et al.*
RSA-155	155	512	$9,383[4]	August 22, 1999	Herman te Riele *et al.*
RSA-160	160	530		April 1, 2003	Jens Franke *et al.*, University of Bonn
RSA-170 [*]	170	563		December 29, 2009	D. Bonenberger and M. Krone [***]
RSA-576	174	576	US$10,000	December 3, 2003	Jens Franke *et al.*, University of Bonn
RSA-180 [*]	180	596		May 8, 2010	S. A. Danilov and I. A. Popovyan, Moscow State University[7]
RSA-190 [*]	190	629		November 8, 2010	A. Timofeev and I. A. Popovyan
RSA-640	193	640	US$20,000	November 2, 2005	Jens Franke *et al.*, University of Bonn
RSA-200 [*] ?	200	663		May 9, 2005	Jens Franke *et al.*, University of Bonn
RSA-210 [*]	210	696		September 26, 2013[8]	Ryan Propper
RSA-704 [*]	212	704	US$30,000	July 2, 2012	Shi Bai, Emmanuel Thomé and Paul Zimmermann
RSA-220 [*]	220	729		May 13, 2016	S. Bai, P. Gaudry, A. Kruppa, E. Thomé and P. Zimmermann
RSA-230 [*]	230	762		August 15, 2018	Samuel S. Gross, Noblis, Inc.
RSA-232	232	768			
RSA-768 [*]	232	768	US$50,000	December 12, 2009	Thorsten Kleinjung *et al.*
RSA-240	240	795			
RSA-250	250	829			
RSA-260	260	862			
RSA-270	270	895			
RSA-896	270	896	US$75,000		
RSA-280	280	928			
RSA-290	290	962			
RSA-300	300	995			
RSA-309	309	1024			
RSA-1024	309	1024	US$100,000		

Troca de Chaves Diffie-Hellman

- Primeiro algoritmo publicado de chave pública
- Sozinho é suscetível a ataque MITM
- Objetivo: Troca segura de parâmetros para estabelecer uma chave de sessão
- O algoritmo depende da dificuldade de calcular logaritmos discretos
- Raiz primitiva → a mod p … ap-1 mod p
- b ≡ ai (mod p) onde 0 ≤ i ≤ p → dloga,p(b)



Diffie-Hellman - Algoritmo

- Parâmetros:
  - q numero primo, α raiz primitiva de q → públicos
  - Xa e Xb números aleatórios < q
  - Geração de chave:
  - Ya = αXa mod q e Yb = αXb mod q
- Segredo:
  - K = (Yb)Xa mod q
  - K = (Ya)Xb mod q
- O adversários só sabe q, α ,Ya e Yb

- q = 353, α = 3, Xa = 97 e Xb = 233
- A computa:
  - Ya = 397 mod 353 = 40
- B computa:
  - Yb = 3233 mod 353 = 248
- A deriva:
  - K = 24897mod 353 = 160
- B deriva:
  - K = 40233 mod 353 = 160

Próximas Aulas

- Prática:
  - Trabalho Individual I
    - Envolve todo este conteúdo que vimos na aula de hoje
- Teórica:
  - Introdução a criptografia e criptosistemas classicos
    - Parte mais difícil da disciplina

Perguntas?

jean.martina@ufsc.br