



CEUB

EDUCAÇÃO SUPERIOR

ceub.br

Segurança Computacional

Professor Doutor
Auto Tavares da Camara Junior
Perito Criminal Federal

Apresentação

- Junior auto.junior@ceub.edu.br
 - Perito Criminal Federal
 - Doutor em Ciência da Informação (UnB)
 - Mestre em Ciência da Informação (UnB)
 - Pós Graduado MBA em Administração Estratégica de Sistemas de Informação (FGV)
 - Bacharel em Ciência da Computação (UnB)

Objetivo

- Reconhecer como funcionam primitivas criptográficas
- Usar primitivas criptográficas corretamente raciocinando sobre segurança
- Implementar e atacar cífras simétricas e assimétricas
- Reconhecer protocolos de segurança para sistemas computacionais e redes de computadores
- Implementar algoritmos de segurança de criptomoedas
- Reconhecer protocolos de segurança de votação eletrônica

Organização

CEUB

EDUCAÇÃO SUPERIOR

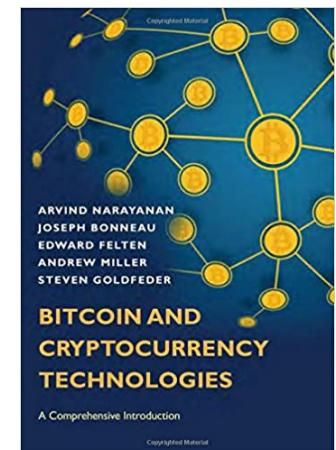
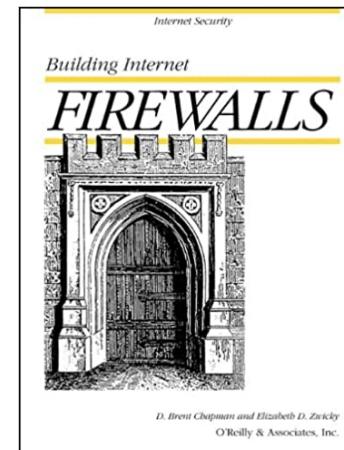
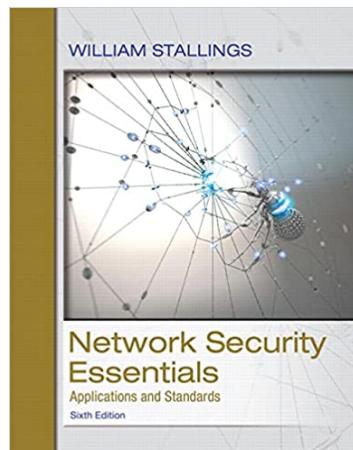
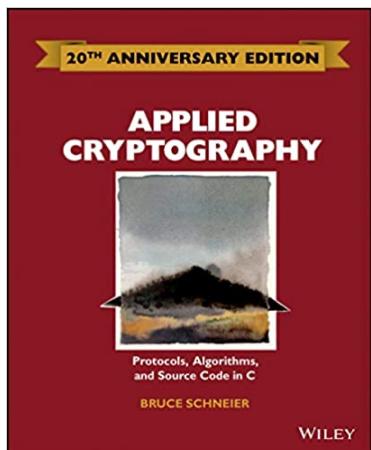
- Aulas
 - Práticas
- Avaliação
 - Conceito (C)
- Nota Final
 - 100% (C)

Agenda

Data	Conteúdo	Data	Conteúdo	Data	Conteúdo
22/02	Apresentação	24/02	Introdução	01/03	Carnaval
03/03	Criptografia Simétrica	08/03	Criptoanálise Simétrica	10/03	Criptoanálise Simétrica
15/03	Criptografia Simétrica	17/03	Criptoanálise Simétrica	22/03	Cifras de Bloco
24/03	Cifras de Bloco	29/03	Garantia de Integridade	31/03	Distribuição de Chaves
05/04	Criptografia Assimétrica	07/04	Criptografia Assimétrica	12/04	Criptografia Assimétrica
14/04	Segurança de Sistemas	19/04	Protocolos de Autenticação	21/04	Tiradentes
26/04	Segurança de Sistemas	28/04	Segurança de Sistemas	03/05	Segurança de Redes
05/05	Segurança de Redes	10/05	Segurança de Redes Sem Fio	12/05	Firewalls
17/05	Criptomoedas	19/05	Bitcoin	24/05	Bitcoin
26/05	Bitcoin	31/05	Altcoins	02/06	Votação Eletrônica
07/06	Votação Eletrônica	09/06	Votação Eletrônica	14/06	Urna Eletrônica Brasileira
16/06	Conclusão	21/06	Conclusão	23/06	Conclusão
28/06	Conclusão	30/06	Conclusão	05/07	Conclusão
07/07	Conclusão				

Referências

- SCHNEIER, B. Applied Cryptography
- BONEH, D. Cryptography Stanford Coursera
- STALLINGS, W. Network Security Essentials
- CHAPMAN, D. B. et al. Building Internet Firewalls
- NARAYANAN, A. et al. Bitcoin and Cryptocurrency Technologies



Introdução

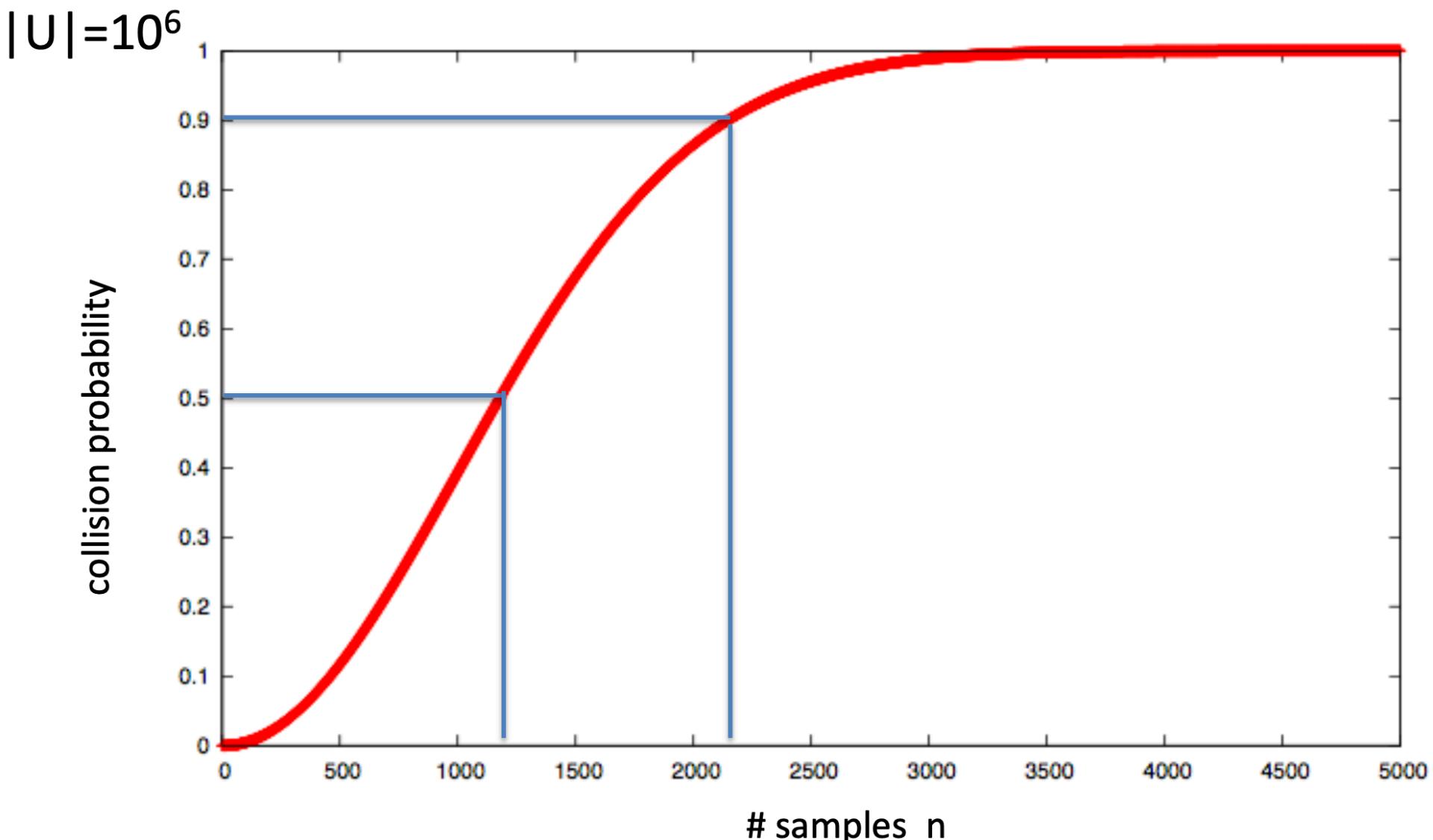
Introdução

- Criptologia
 - Criptografia
 - Criptoanálise
- Fundamentação Teórica
 - Matemática
 - Estatística

Introdução

- XOR (^)
- Teorema: paradoxo do aniversário
 - Sejam $r_1, r_2, \dots, r_n \in U$ variáveis aleatórias independentes identicamente distribuídas
 - Se $n = (1.2 * |U|^{1/2})$, então $\Pr[\exists i \neq j \mid r_i == r_j] \geq 1/2$

Introdução



Introdução

CEUB

EDUCAÇÃO SUPERIOR

- ASC II
- Hexadecimal

Introdução

- Criptografia está em todos os lugares
 - Comunicação segura
 - HTTPS
 - WEP
 - 802.11i WPA2
 - Bluetooth
 - Segurança de discos
 - EFS
 - BitLocker
 - FileVault
 - TrueCrypt

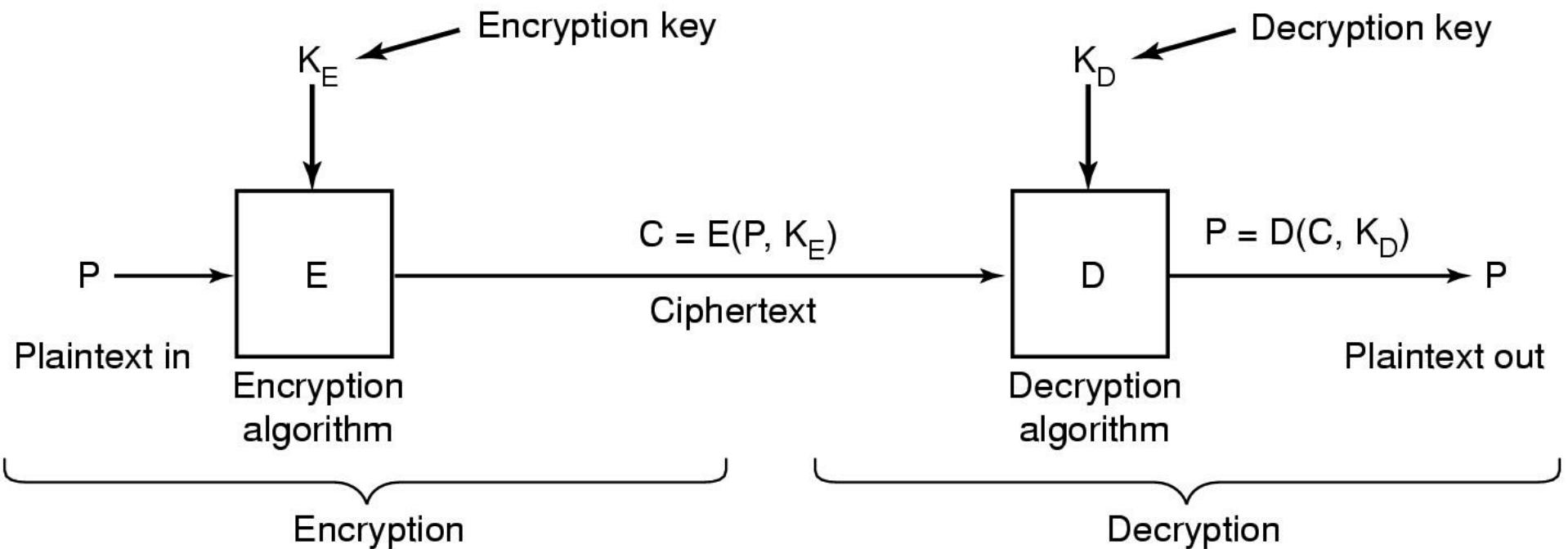
Introdução

- Criptografia está em todos os lugares
 - Proteção de conteúdo
 - DVD
 - Blu-ray
 - Autenticação de usuário
 - Assinatura eletrônica
 - Dinheiro digital
 - Votação eletrônica

Introdução

- Rigor científico
 - Especificação precisa de um modelo de ameaça
 - Proposta de construção
 - Demonstração de que a quebra da construção sob o modelo de ameaça resolveria um problema difícil subjacente (NP ? NP-Completo ?)

Introdução



Introdução

- Passos
 - Estabelecimento de uma chave secreta compartilhada
 - Codificação usando a chave secreta compartilhada com garantia de confidencialidade e integridade

Introdução

- Criptografia simétrica
 - DES
 - 3DES
 - AES
- Criptografia assimétrica
 - RSA
- Algoritmo de encriptação deve ser publicamente conhecido
 - Nunca (!) use cifras proprietárias

Introdução

- Criptografia é:
 - Uma ferramenta extraordinária
 - A base para muitos mecanismos de segurança
- Criptografia não é:
 - A solução para todos os problemas de segurança
 - Confiável se implementada ou utilizada inapropriadamente
 - Algo que você deva inventar você mesmo: há milhares de exemplos de projetos ad-hoc humilhantemente quebrados

Introdução

- A ordem mundial depende da criptografia
- Segurança é a área da Tecnologia da Informação mais bem paga
- Guerra nas estrelas (Luke Skywalker X Darth Vader)

Introdução

- Programa cifra rot13

Criptografia Simétrica

Criptografia Simétrica

- Definição: cifra simétrica
 - Seja um conjunto K
 - Seja um conjunto M
 - Seja um conjunto C
 - Seja um par de algoritmos eficientes E e D, tais que
 - $E: K \times M \rightarrow C$
 - $D: K \times C \rightarrow M$
 - $\forall m \in M, \forall k \in K: D(k, E(k, m)) == m$
 - E pode ser um algoritmo não determinístico
 - D é um algoritmo determinístico

Criptografia Simétrica

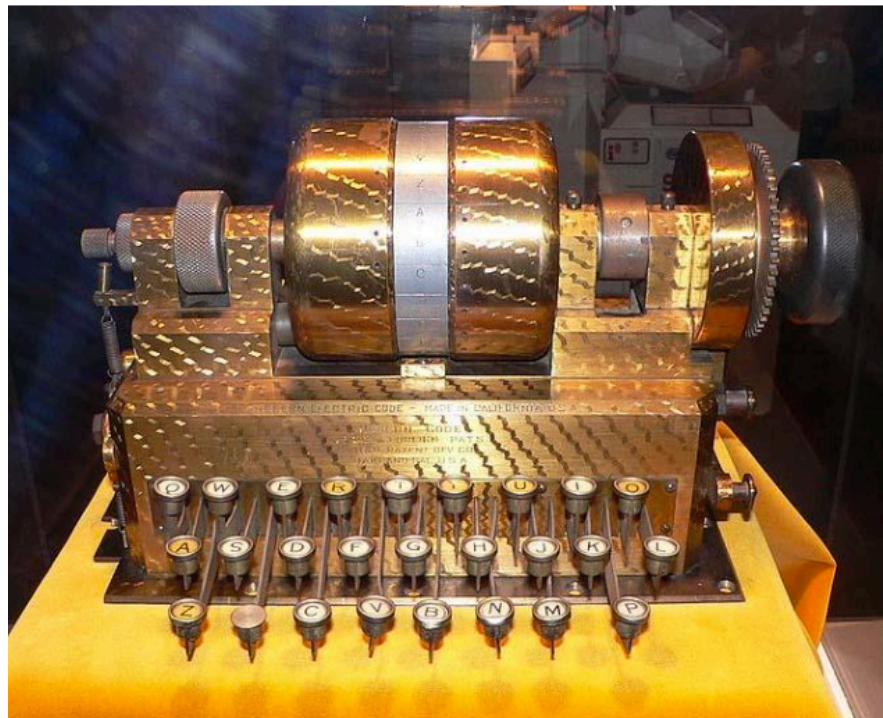
- Cifras de substituição
 - Tabela de substituição
- Cifra de César
 - Aula de criptografia do Junior
 - Bvmb!ef!dsjquphsbgjb!ep!Kvojps
- Cifra de Vigenere
 - $c = k \wedge m$

Criptografia Simétrica

CEUB

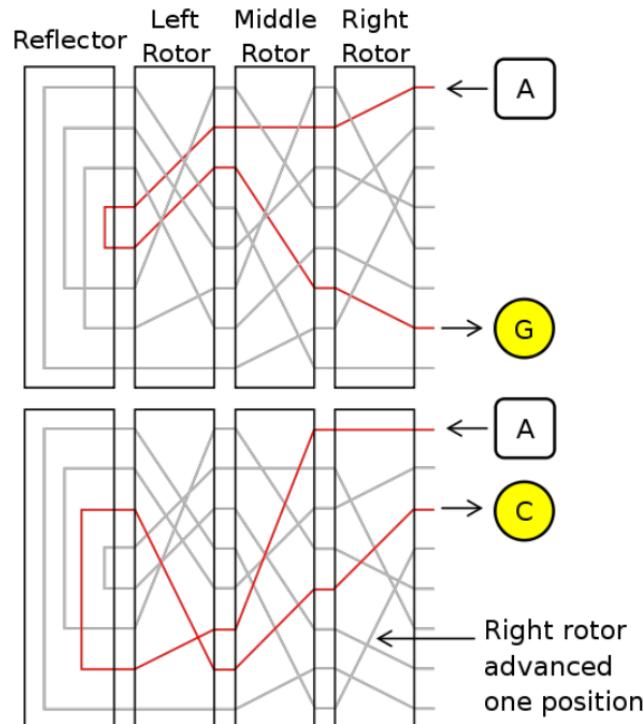
EDUCAÇÃO SUPERIOR

- Rotores
 - Máquina de Hebern



Criptografia Simétrica

- Rotores
 - Enigma



Criptografia Simétrica

- DES (1974)
 - Data Encryption Standard
 - 2^{56} chaves
 - 64 bits tamanho do bloco
- 3DES (1995)
 - Triple Data Encryption Standard
 - 2^{168} chaves
 - 64 bits tamanho do bloco
- AES (2001)
 - Advanced Encryption Standard
 - 2^{256} chaves
 - 128 bit tamanho do bloco

Criptografia Simétrica

CEUB

EDUCAÇÃO SUPERIOR

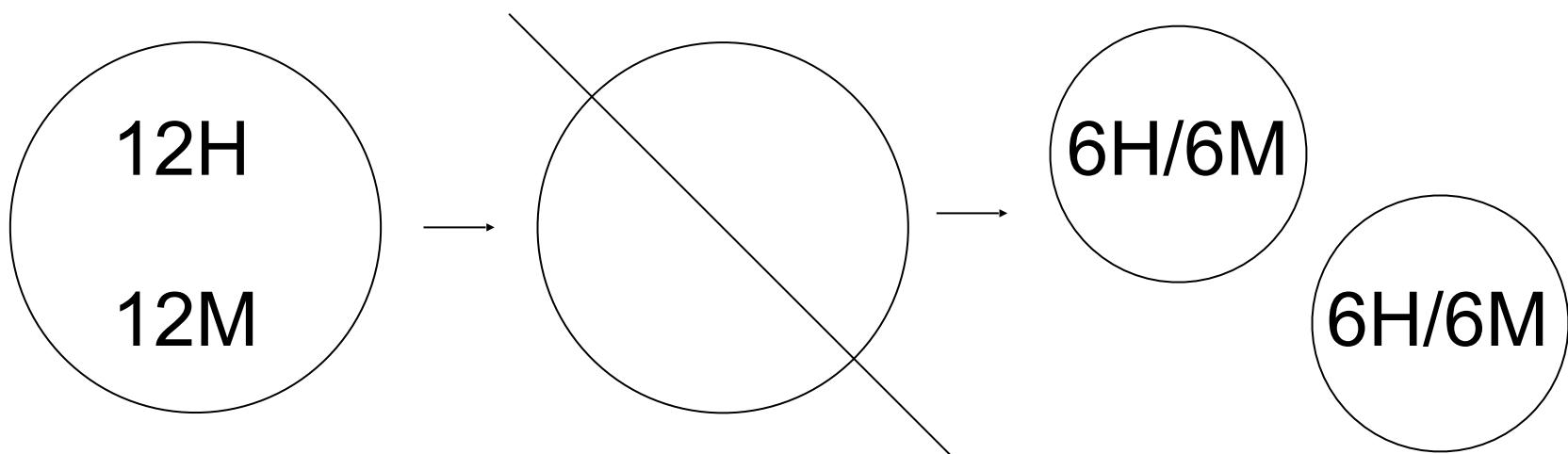
- Programa cifra de Vigenere

Criptoanálise Simétrica

Criptoanálise Simétrica

- Criptoanálise de Vigenere
 - Fundamentação estatística
 - Ocorrência de caracteres
 - Bvmb!ef!dsjquphsbgjb!ep!Kvojps
 - Caracter que aparece mais vezes : !
 - ! → “ ” qual a relação ?!?
 - $\text{Asc}(!) = 33$
 - $\text{Asc}() = 32$

- Criptoanálise de Vigenere



Criptoanálise Simétrica

- Dado o criptograma:
 - 2b0002084f160f550d1b06021e1a091b0e1403144e0d0052208f00000000
- Suponha uma chave de tamanho 6

0	1	2	3	4	5	0	1	2	3	4	5	0	1	2	3	4	5	0	1	2	3	4	5	0	1	2	3	4	5	
2	0	0	0	0	4	1	0	5	0	1	0	1	0	1	0	1	0	1	0	1	0	4	0	0	5	2	8	0	0	0
b	0	2	8	f	6	f	5	d	b	6	2	e	a	9	b	e	4	3	4	e	d	0	2	0	f	0	0	0	0	

- Qual a probabilidade de, com a escolha do tamanho da chave certa, encontrar-se um caracter que seja muito repetido ? Encontrado tal caracter, qual a relação dele com o original ?

Criptoanálise Simétrica

05551b5f59310f200c11d9523f186e555f016a05275e5e172307214210162f552b5f4
31b241a6e5f515229143e58441326552a5e10022b983d1f103b24143b5645002b11
2111531d271a6e72551c3e0721154176a302042591c25551b5f591423162f555f52
2e106e73421339982258515267550d7465306a102311014b7c4d6211441d381b214
41d012f552111400023182b58421d6a162b5f440025553b5f59042f073d584493381c
211154136a072b565991255520501016a3162f5551522e106e0800522f553e504301
25006e50101122142350425f39106e72551c3e07211651c23032b43431b3e943c5
85f522e106e73421339982258515267551b5f59310f200c1f103125186e545e01231
b211154176a103652551ea01b2d5851522f553e5e5c9f3e1c2d5010162f553c545e1
d3c14a9d25f523a103c5c511c2f1b3a541c522b55275f430623013b58d79125552f52
5f1f3a14205951522b066e54461d2600a9c455016a012b525e1d268629585313395
52b1140172e1429c2571b29143d1f103d6a20205873371f376e5e561738102d54101
13f073d5e435224143d11d1002f143d1154176a1627db5e1123143d115a0738982a5
8531339596e525998241627504352391a2d58511b39596e5259982416275043522f
0d2f45510166552d58da1c291c2f4210162b553d50ca162f596e5259982416275043
522e146e5454072914a9d25f522f553a54531c25192156591366552f5dd91f6a1121
4210113f073d5e43522e106e41c30167123c5054072b92ad5e101e2b01211155523
9013c58530625553d545e013f5b

Criptoanálise Simétrica

0053270f21331264022261252d01222f9b360367a853310b672c9a3009232e5320036722012d16332
e14360721281264173224533115266106290767329a360f22611721462328152114222f0721156722
1a2214263253200367029a3707356112515222017251567241e640a223501251567251664132a20
5337032929126a4613331230076a3216640222610629076737163615a42e53370f2a311f2d002e221
2200767251664132a205329072e3253230335201f64052e2701254623245337132532072d1232289
4a70967311c280f262d152504ae351a27076b611a2a10222f0725022661032b14670d162b08226131
2512332800300767001f260335351a64052233102546232453755271745d642767281d320329a690
2b46232053270f21331264022261252d01222f9b360367a8532114352017250b222f0721462635012
d0432ac17254626613128072e321664022261252d01222f9b36037c61162a05282f0736076a321664
093528142d08262d1e210833245320033422012d122661032b1467061a2b10262f53060733280030
076703162807342e532a0967321631462b280536096725123007232e532003677046715567221c29
46286107a912322d1c642a2661102d0035205320032b6f53170f206f53030f2837122a460520072d15
33205306032b20002b48670400300767221a221426619a640b3228072b46242e1d2c032428172546
372e01351322619a6400a6221a2846232453340335221626033561166402226103b01467241e6416
35a0072d05266d5334073524102108232e5f6407673006210b6735162946372e062707673101a512
2e22126846363416648f67281d3513222301a510222d536c0f292516270f21339232032b685d64252
82f00211732241d30032a241d30036b611e310f332e006416352e1436072a20172b142232532d0b37
2d16290329351236072a6116371732241e251567251664053528033009203312220f26611d251567
32062515672003280f242094b10334610231036732902b46292e53211534241d270f262d53270f213
3123746232453120f20241dac14226d5321463634166415a42e53220724281f290329351664173224
11360723200064162833533513262d023103356110360f37351c2508262d1a3712266f

Criptoanálise Simétrica

Criptoanálise Simétrica

3e11335715520040105c125c115c52501411275d09de115d10113157015600551d115a122163341851c20555865c524414431a530b561c40141d5757164317579c571e510a13015d1f56025e04415e141e4310530b5a0855155e5757455e135a0558135d454317581011225c0cd01d18515457571647004105440553015c52511c1114531741175d03505b12065c1f141044035d0b5c1f5d1011184082521f511f4596400c25e1410551a5b0b5a01400350035b1352525151571e5c045d11511843161e45571b461445165f005d0651514202500a41165d1f50135d45521d143c58195b1647005b5155121220400655155e57560413384102451ed5041f5240145c57420a415252185f165e0c5713501411124a00411151031d57570813065b155e575d45471746035803c1175a1d141f50145b0a5d13585d111641455206461853025b82c6174751410557135a01401042575c0a13d514408157560a131346051f5703510752501011345d0b40065d05441ed5865c527214551240045f5e141f5e579545041d14155e575317475c144306575604133e51181195d4502421a4709441e455717144309575600131f55185e57560013400441025757491317470154145b035a11551c5419460009527d511c57531546005503111e5c034113d38454041215561c55184257510a5d0646101116120a4116511c11075d09de065d1250575745401d5718501b120a4652511c11135711411b59145f035d45571714135419414913015103471ed50a405251515819460041174702540412015252611f58945d455c07141554574110520114145f035b015216510211164711d200450458145316131714145c07400040134751418d50095a1155021d5750005e525502421e5f455c0740035004120c5d144610d68257161311411b50574217d2065d12505746005d1a5551431242004111410242945d455a1c401443124111521641105d575d10131b5a0554055c04501b5b1f501b120013174c185b161217560246144204d10a13075a1857184008565e14025410470b571d14025457560c40024102540512005e525814584c122c7a52195141055713561c5d0311121217560246185c1e40455c524003d0115b065c525d1ddc145b115c52501411125c115c00441452125c11560114141113400a5413475150115b0b405e141e11145d0b470055135019560a1317141e11135716501359185f1f5d455717141354194145565242105d184000405e1402541a121541175e04dc0d5d4557131410d6945d4555134e145f13d3175a131414111357455c0740035e0412964115d71e4257429f511e5d125e04120b520114035404420050065d07500412844117550211135745501d59015403d80b501b554a113e7b2c135f14144912400656001410425754105d95c1144257560013025b1ddc145b04131f5503dc035b08525e141054055d155c004004d0055b0413171415545754175c1c40145805531608527d27115a12004b17461254051e45501d5951540f510946015d0758135301565e1410425754105d95c1144257560013025b1ddc145b041318411558145b84411b5551551612305d1bd71e0a5764451e52571e58155b171313140544055004d4915b5154575d45560156045d1f5d45431d470254044196411b5b515518414551175a02111212015c011401439e560c5c0114155057670b5a915b51545756044052511f451e560457174751581946005400551f4512414557131410551a5b0b5a0140035090d10a1302ce135d1e510413145115540553091f5247145c5742175618419c4b181201525259105f0246005d95d71e111353455c0050145c57429f511e5d12505742005f13475161185e88501b5502113a5b095a065503540412015c011434420353015c010f515457642c135f141052185f15521c5c10435757455a1c47055002400441525d1f4002db175a065b021105570952115d1e5f16560a4052551e4257510a5d1458184518414552154690431e5d16131d415157025c015a9346185e041200131d475155125e004052501452184017561c4014425b121446135a155e574100130646104516404557171412431e5f001316515152185f155606de1f521e53455517501443165e491310511c111641165a1f1401431244005d1b46515457400043005d1c58051200400151021114400c5e17475f

Criptoanálise Simétrica

1a1d492209120d27071d2e0a0642310b49200d1414304e1a2a089c1627070a22455d1634030baa0855013d0f0422
011a11750a0c63361c11210b0422165506304e2a2b040307753d002e8c01103c0d086f4516103c1e1d2c020703330
70863011042360608350055983b070a2249550d204e0a310c05163a091b22031c03750a0c63061d03230b493000
1610301a086a4506813a4e1c2e045501390f1a30005506304e082f021a103c1a042c165512341c08630455012707
19370a121034080022495513200b493616140f750d0122131011750d1b2a15010d321c88250c1603264e1b260914
013c010722011411751e0831045503264e0633000703b29b0c30451107750d00251714053003492645110736070f
3104120738404902451a12301c08a4861a42310b49200d1414304e1a2a089c1627070a22459c42380f003045060b
381e05261659422501003045050d310b49261d1c1121071b631018037594072a061442360608350055073b1a1b2
645141175011926171485a00b1a6d453442360608350059423b0f49331794163c0d086f450707251c0c30001b1634
4e1c2e450607321c0c270a5942250f1b370c190a340a0663001b16270b492710141175011c6308140b264e192217
01072642493210104225010d26085511301c4936161406341d49330407037503082d111010751b046306140c3402
49200a1b043c0a0c2d061c03394e0d26451c0c33011b2e0492813a40491616144f260b4936081442af00002004550
13d0f1f26495512341c1d2a091d03310f49330a074234030b2c16550d264e002d11101039010a36111a10301d4563
0b1442251c0c2e0c0611344e0d26450417304e0c30111442bc4e0a2c0b1d0736070d22451412300083045050d27
4e0c2f00064c75211c37171a11751a0c31081a11751e0831045501270719370a121034080022451107750d012213
1042260704aa11070b360f4930861a58750d1b2a15010d321c08250c1442310b49200d1414304e1a26060707210f
4563011042360608350055983b070a22495506304e0a2b040307750d062e1514102107052b041103794e0d26450
00f344e0a2b040307750b49270055013d0f1f264505103c180827045b421a4e1c300a55063a4e932f111c0f3a4e1d2
617180d751e0627005582264e1f261f1011751d0c63061a0c331b07270c0742360104630a55013a03192c0b100c21
0b49200d1414304e19310c0303310f4927045501270719370a121034080022451107750d012213104225940b2f0c
16037b4e286306070b251a06241714043c0f49270055013d0f1f2645060b38871d310c160375874933040703751d0
c31450607250f1b22011442310b4920171c1221010e3104130b344e0d2645160a34180c630406113c038037171c0
13440

Criptografia Simétrica

Criptografia Simétrica

- Definição: perfect secrecy
 - Seja uma cifra (E, D) sobre os conjuntos (K, M, C)
 - $\forall m_0, m_1 \in M$ que $m_0.length() == m_1.length()$
 - $\forall c \in C$
 - Se $\Pr[E(k, m_0) = c] == \Pr[E(k, m_1) = c]$, então essa cifra tem sigilo perfeito.

Criptografia Simétrica

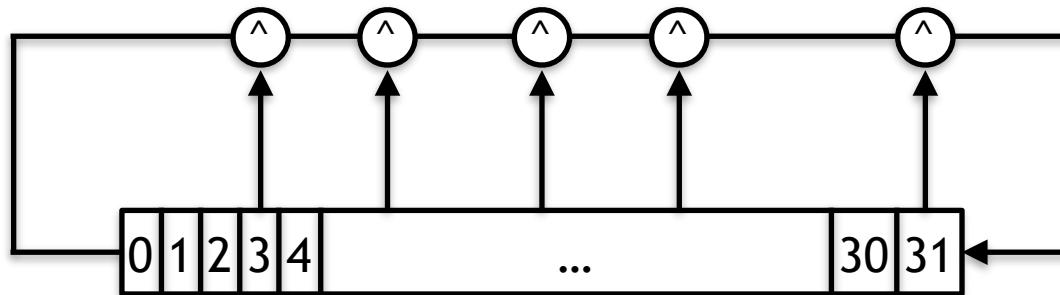
- One Time Pad (OTP)
 - Cifra de vigenere onde a chave é do mesmo tamanho da mensagem
 - $c = k \wedge m$
 - Por extensão, $k = m \wedge c$
 - Muito rápido para encriptar ou decriptar
 - Tem sigilo perfeito (!)
 - Difícil de usar na prática
 - A chave tem de ser muito grande
 - A chave só pode ser utilizada uma única vez (!)

Criptografia Simétrica

- Pseudo Random Generator (PRG)
 - Forma de usar uma chave pequena (senha) para produzir uma chave grande (OTP)
 - PRG deve ser imprevisível
 - Não utilizar as funções random() das linguagens de programação

Criptografia Simétrica

- Pseudo Random Generator (PRG)
 - Linear-feedback shift register (LFSR)



- Pseudo Random Generator (PRG)
 - Linear-feedback shift register (LFSR)
 - 3 registradores
 - 1 cabeça
 - » Sempre sofre deslocamento
 - » Define qual gerador vai ser deslocado
 - 2 geradores
 - » Tipo 0: $\text{xor} = r[31] \wedge r[6] \wedge r[4] \wedge r[2] \wedge r[1] \wedge r[0];$
 - » Tipo 1: $\text{xor} = r[31] \wedge r[6] \wedge r[5] \wedge r[1];$
 - » Definem um bit cada um
 - » Xor deles é o resultado pseudo randômico

Criptografia Simétrica

CEUB

EDUCAÇÃO SUPERIOR

- Programa LFSR

Criptoanálise Simétrica

- Casos reais
 - Microsoft Point-to-Point Tunneling Protocol (MS-PPTP)
 - 802.11b WEP
 - Criptografia de disco

Criptoanálise Simétrica

- Criptoanálise do OTP
 - $c_1 = m_1 \wedge \text{PRG}(k)$
 - $c_2 = m_2 \wedge \text{PRG}(k)$
 - $c_1 \wedge c_2 (?)$
 - Crib dragging

Criptoanálise Simétrica

- Criptoanálise do OTP
 - Criptogramas em idioma inglês

Criptoanálise Simétrica

315c4eeaa8b5f8aaf9174145bf43e1784b8fa00dc71d885a804e5ee9fa40b16349c146fb778cdf2d3aff021dff
f5b403b510d0d0455468aeb98622b137dae857553ccd8883a7bc37520e06e515d22c954eba5025b8cc57e
e59418ce7dc6bc41556bdb36bbca3e8774301fbcaa3b83b220809560987815f65286764703de0f3d524400
a19b159610b11ef3e

234c02ecbbfbafa3ed18510abd11fa724fcda2018a1a8342cf064bbde548b12b07df44ba7191d9606ef4081ff
de5ad46a5069d9f7f543bedb9c861bf29c7e205132eda9382b0bc2c5c4b45f919cf3a9f1cb74151f6d551f448
0c82b2cb24cc5b028aa76eb7b4ab24171ab3cdadb8356f

32510ba9a7b2bba9b8005d43a304b5714cc0bb0c8a34884dd91304b8ad40b62b07df44ba6e9d8a2368e51
d04e0e7b207b70b9b8261112bacb6c866a232dfe257527dc29398f5f3251a0d47e503c66e935de81230b59
b7afb5f41afa8d661cb

32510ba9aab2a8a4fd06414fb517b5605cc0aa0dc91a8908c2064ba8ad5ea06a029056f47a8ad3306ef502
1eafe1ac01a81197847a5c68a1b78769a37bc8f4575432c198ccb4ef63590256e305cd3a9544ee4160ead4
5aef520489e7da7d835402bca670bda8eb775200b8dabbba246b130f040d8ec6447e2c767f3d30ed81ea2e
4c1404e1315a1010e7229be6636aaa

3f561ba9adb4b6ebec54424ba317b564418fac0dd35f8c08d31a1fe9e24fe56808c213f17c81d9607cee021
dafe1e001b21ade877a5e68bea88d61b93ac5ee0d562e8e9582f5ef375f0a4ae20ed86e935de81230b59b7
3fb4302cd95d770c65b40aaa065f2a5e33a5a0bb5dcaba43722130f042f8ec85b7c2070

Criptoanálise Simétrica

32510bfbacfbb9befd54415da243e1695ecabd58c519cd4bd2061bbde24eb76a19d84aba34d8de287be84d0
7e7e9a30ee714979c7e1123a8bd9822a33ecaf512472e8e8f8db3f9635c1949e640c621854eba0d79eccf52ff
111284b4cc61d11902aebc66f2b2e436434eacc0aba938220b084800c2ca4e693522643573b2c4ce35050b0
cf774201f0fe52ac9f26d71b6cf61a711cc229f77ace7aa88a2f19983122b11be87a59c355d25f8e4

32510bfbacfbb9befd54415da243e1695ecabd58c519cd4bd90f1fa6ea5ba47b01c909ba7696cf606ef40c04af
e1ac0aa8148dd066592ded9f8774b529c7ea125d298e8883f5e9305f4b44f915cb2bd05af51373fd9b4af5110
39fa2d96f83414aaaf261bda2e97b170fb5cce2a53e675c154c0d9681596934777e2275b381ce2e40582afe6
7650b13e72287ff2270abcf73bb028932836fbdecfecee0a3b894473c1bbeb6b4913a536ce4f9b13f1efff71ea3
13c8661dd9a4ce

315c4eeaa8b5f8bffd11155ea506b56041c6a00c8a08854dd21a4bbde54ce56801d943ba708b8a3574f40c00
fff9e00fa1439fd0654327a3bfc860b92f89ee04132ecb9298f5fd2d5e4b45e40ecc3b9d59e9417df7c95bba410
e9aa2ca24c5474da2f276baa3ac325918b2daada43d6712150441c2e04f6565517f317da9d3

271946f9bbb2aeadec111841a81abc300ecaa01bd8069d5cc91005e9fe4aad6e04d513e96d99de2569bc5e5
0eeeeca709b50a8a987f4264edb6896fb537d0a716132ddc938fb0f836480e06ed0fcde9759f40462f9cf57f45
64186a2c1778f1543efa270bda5e933421cbe88a4a52222190f471e9bd15f652b653b7071aec59a2705081ff
e72651d08f822c9ed6d76e48b63ab15d0208573a7eef027

Criptoanálise Simétrica

466d06ece998b7a2fb1d464fed2ced7641ddaa3cc31c9941cf110abbf409ed39598005b3399ccfafb61d0315f
ca0a314be138a9f32503bedac8067f03adbf3575c3b8edc9ba7f537530541ab0f9f3cd04ff50d66f1d559ba520
e89a2cb2a83

32510ba9babebbbbef001547a810e67149caee11d945cd7fc81a05e9f85aac650e9052ba6a8cd8257bf14d13
e6f0a803b54fde9e77472dbff89d71b57bddef121336cb85ccb8f3315f4b52e301d16e9f52f904

Criptoanálise Simétrica

- Criptoanálise do OTP
 - Criptogramas em idioma português

Criptoanálise Simétrica

9d8ede898dadac322c34dcc2388976a44e52f6880ce89f4777e087982e00cd56ece7c9ae41770ccf01167c92
31e90a86517420ed318658884c788570374769092d9f406c21b375583c42a0bc6b26fde6119bf677dcf90193
88ccb5d7f309f69ca5690c0c6fcbd14ca4490810bae92f0e3ec7ac0a6a27ebba087c18dac3cd3d606b0102f48
f67a817f5fcaca3e2e5b56cd0c233968a9afa878414e77b0cf2b31f881f5777cd8b265762585f90f08947

81cbfa9991b8b0ba6d41d6ce6e8f6bba5753639b01e8cd4661e0aa9f6f104958e0f49a22067713cf4f9873c1a
ca01fd348e1acf67405dec7097293392a413a0e3d82446d68b862582f4cbfb87731e9ee1f9bf676c1f6068885
8eaecae747b9dfa5710c1b6bc1db1fe1454772a0e92e8725cfbf436669f7f52a611ccfc3c169603e6703f18e7a
ba5bb0f5e9b4ff7cfb66d2c030cf9d8fa878435fa77103fbe5680514632eb983452e4cf59def89d49e064d969
82def59ce75b6589f5812b1660298e3b441c3f98cd36543c2945f73e5a03117cbc33296e

91dcf49c97b6b92f6d07dbc6e0524b8074578940ff2d1577de0a18f6f035253ebe50437086d128e445f66082
6ee179059e0e3e77c924fcd4e7792782a08391b2a8e057d21ba75193e03b3e86736ebf8199db7398eec1d8
88a4ff1c9f305bf91a36a581a66c6d381b7414472b8e92e8272c1be063b3ce1ba22f6048ec5c127672a2a47f1
8970ba08bab96cb3adefba61c7ca2d040cdfeccac739f8781671be12884c1c

87c3fccc8db6b7296941d6ce3d9865a40b0661930be3d00376a1e5892617415ee0a69926136341c1013a7c
8620ee169c18ddacf47ece1dcd477599772d5a2c137881507368a8751d2103b6a92206ede4049bb7798eed
1fda96cfacc4e805b78ebf6d0c1b658fd60da8565a3de4a82d96378ea8536a2aebf4247008389de842d6a6b3
10ee39e74e91ef5fde9e0eee0f47fd43ae36cdd9f9ea87d424fc771a71ab199c125f32b5ca32476d58598bba9
b0ca460c52680d2391d2f75fa207f3cc635975689131434a321e8229012c7c45f73c5a025f74b6382d33cb9e
c302c044ccc5e143d775068074eecb3e394d3a36c1dcae3fba448ac8222b44ce27

Criptoanálise Simétrica

98cfb8dc330fe28610092c7278263a24641729745e3da0362b2aa8d3d124d5b626586670e7008cb4f0b738
524a01fd357f1a9e7658d4e884d73857c375e26162e86417f68b2665828cab1a96624a8ee15c9ef258ee81d
88c4dbb1c4b240a78aa374495f6eca941cb34b4f20a9e53d873ddca8556a2aecff2a7c0acad084396039672d
f18770ba5b92f6fface4e6f22391c122c39cd7ef98c125f43a2c6ab156a4565125f699385177495b8db9c82ce9
219836c08fb09db370e31cfb8129167a299c3a471f3f0dcbb211b6d2c45bb3915141269ad3337219fa3de108f0
8ccc5c34fc467068735e8c7323e17

9ccfb828cb0aa382c05d7d83a8d24a65247658e04aad9467bb2a4c66f120079c7c0c9260f770fc481067c1
34f51bdf18f2e3f2709049c15b369276796b2817288a4a7029a868580e51b3bb6b29ede30286f671cbb840ca
d69ff085fa44a09ab8e50c0a678fd805ac4d5c37e8f83d91338eac063e3bebf92d350fcb91d0a06c252e04ff99
35ad1ebbedfeafadecf42fd2c02e939cce60d4739bb3a3c7ebb17c94b5b3afcca32d1235c599af29a88a465cf
6b99c3f980b34fef4aeed32a107d6899314451761cc321156d2852b2315b101b76ad7637b39f9cc315891648
c5f045d27e1bd530f9c334234ab83785d6a333ac1789c0392a0bd27c1edc1f38730604104b4444e6155c8aa
d22

98cfb8dc330fe3c2c08dec32fcc69b64e55378a0af7ca4f7db3a4ca2b1c0057f0e88d28416741db4c1e32852
4f35e815df4aa7774911dc5487f85393d4d2709398240703cb927082355bda96624fbaa1486f665c2f91c9f90
cff285dc4af68fab775f1e6ec0940aae4d083de8eb398d26dca2062e2ca4ea23710edcded7267c6b2e0ae003
67a014a6b5aca5adf06291da2ec389dbef8fc876e5681a6fb0188d5a4036f79e24026d4d1688fe8c08a471c
56a1dc3f991f216a209efcd3b0c6168917e534a331cccd2b80203543b67851105f50b1322b2e569fc510c2

Criptoanálise Simétrica

97dbbd8f82b7aa322c11ddd93f9961f748067e9416f3de4d66a5e58f371a534ee0a68c6700220cc74f1773c13
3e91a9218f6b0f6f0c25ec744669a7c2d49675a160c4a3e3bb372582d4fb7af7020a8e41584f666c1ed528e9
6c7afd1f71ff68ca5710c0f65cac00def046120a56b33c336cfbe062926ede92d664bc8c4c3206b222614bcc
7b2a14f5eae5aef9e7b568ded52cc397dff2cad039e7771a71ab19c71f7323eb8b3747705f59def98700f064d9
269597f49bf249a204f581391c7d7d9270

938ede838eb0ad2eef0e92e6279f70b6074272da2af558427fa5ab9e20534455a5c58629067004dd521032af
24e3179c56f2afae318152c55979856d380839152acf417b38a97319284ca1e86765fbef1e88b27adcfd01d6c
4cfacd7fd53b98aea6a490c7ece941db44d4626a9a53a863bdcac06627bb1b36c7a4bdec3cb236a3f2847f48
f35a51ebcb9e8afadc7e7e8d0c2268d8dd5bf8ec576c07416fc056995e4036b9d871103200169df88549e57
28a7495d4f59be75bf14aff812e0a336d982d460f251ed165043f3956be2b41100c39af3736219f89df058944c
88bef0e

938efe9e8aa9aa326d0f53c7279f61f7ce0676da04f5cb4632a4a0ca3b164e4ee4f4c923047102c1430d7b936
5ef5e875debb7ed318154ce5b779276794d66152dcf443e242f60112f42f2bd762ce4e30a88b2748efd1fda97
dbbd85f74bb58da374581eed4cdb4ce9474033beed75cd

86c1f98390f9b12e2c05dbc3dcc75a24648739545e6dc4c60a4aac46f3dc355a5f28c29096d41c3401661c1
2aa00a9655e3aca2609758885977856a365d675a158e563e3cb969102303bfbd6b31e7aa048cbb65c1b652
ae81c3b3d6b251b99ba524435f7ecad91cae044c3de8e5298d36c1e3061e26e0f53f3504dd91c0206e38670
6fe9e70ba5bb1fcaca4e2faf866c38f2f8694d8ed858433b57f0c6eaa130e501234f6872e0265435fdef8c80de
d6084

Criptoanálise Simétrica

94c7ef8994b8b2312c8892de238d24a4484a621d86e89f4777e0b68f2806525beb618867036312cb401b73c1
20ed5e9b59e1a7f5709058884663d66a364e3d0d399d403e60b166113f03b1a76f30e5a35098a37082b813d
a94cfaed1fb57f69baf2459122accdb02ab514626a7a8388672dca8413828f7ba23604bc7dfd73d7d3ea092f59
939e91abbf8e0a9fee9b56091db31029fdff8858432f03a0d7abb13c94f5325f8ca254777494493fe8608f621db
7391dee3d2fc4ae718fb46ba1c6029993b161e241ecc3619242f533437151e0a39ad332725cf0b4f1ecc00ccc
5e441d2781ad524f3ca383d19283dd793e62aba0789d9313c4ace27

9d8eeb8580bcf32d7e04c1c22a896aa342065f9b08eed3577daee5a7200652d9eaa68d22026e00dc4e0a328f
20f30a9218e2b6eb7f965c854f739f6b380861486dc6093e2db1271d2257a0ad742cfbfe11c9b87a8ec813960
5cdb5cab241b9df9a684d116bc3c003ed045927ada833c33c54a0433826a4fe293506c1c3d02c7c6b3708e2c
a56a60dbcfd1f1b4a8fb6091ed31828ad3f3ca8323f96e0d7eaf179a4c5d22b985614e6a415f8af2c80deb21c
8699d97e397fd49ed4db4

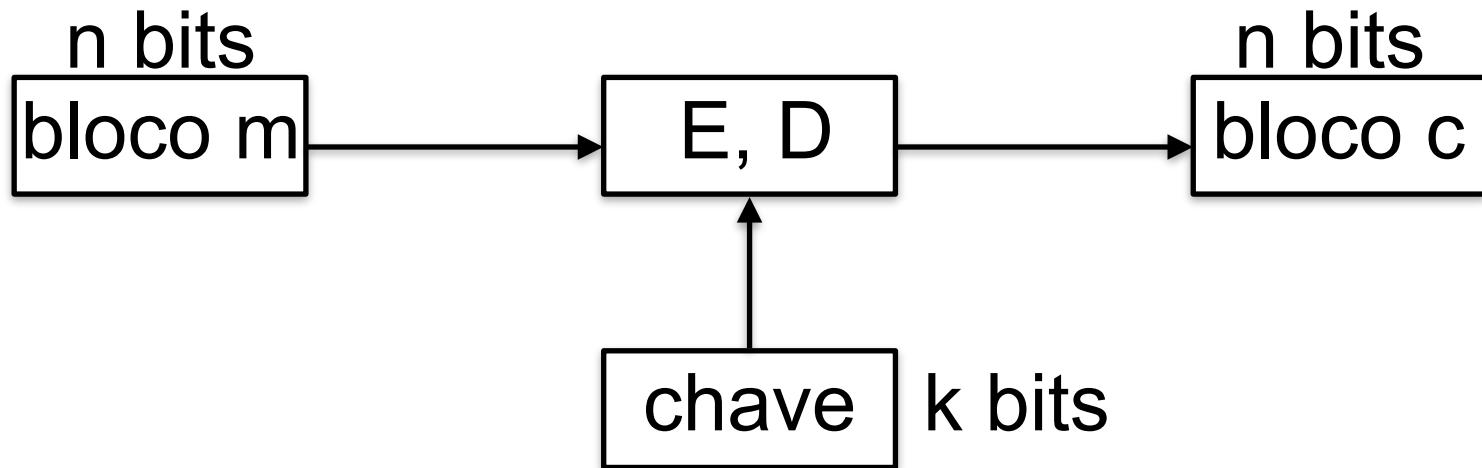
938ef0858db1bf7d6d0ddfc6e98e5f746547a9b01e69f4632a1b5852107415ee4a69926136341cf011c73932
4a01a9c18e0acf162875ac70736a676305b690a3995056d2db1270e2359f2b8633fa8f91584f663c1e2529407
c1fc4cb255b785eaed0c126fcfdb42e1655b72beed2686218ea8536a2fe5f6233508c1dc84282f3d2e03f1c435
8808f5efe9bae8fbb5e691ca2f82d9cbea8fc976f1730531ff279c5e5e77f8ca3143790c478bf2c80cf121c4e59f9
7e187f648ed4af9ce210a767b8b3f444a261ed0245439394ea33947510c7cad762225d385d65f

82cfef8d8130b02e2041c1ce3b9f24a14641769810e9db4c61e0e4ca1e064557a5e58629126706db480a3290
30e51c8159e1e3f67e8652db0973d67a314d2e1b2acf446aa1fc6609394af2212235e7f8019cb33547b814958
0cffcc8f756bb90ea250c3e6dc0c60de142493ea9a82c91338ea04f2773a4f93e7c1bdadec33b6e2d2e06b003
35a85bb6f6e5b3eca8f86ed8dc638f9cddfe868432f0690c7aff1b9c515638b5ca2e572342d591b70149bb2095

Cifras de Bloco

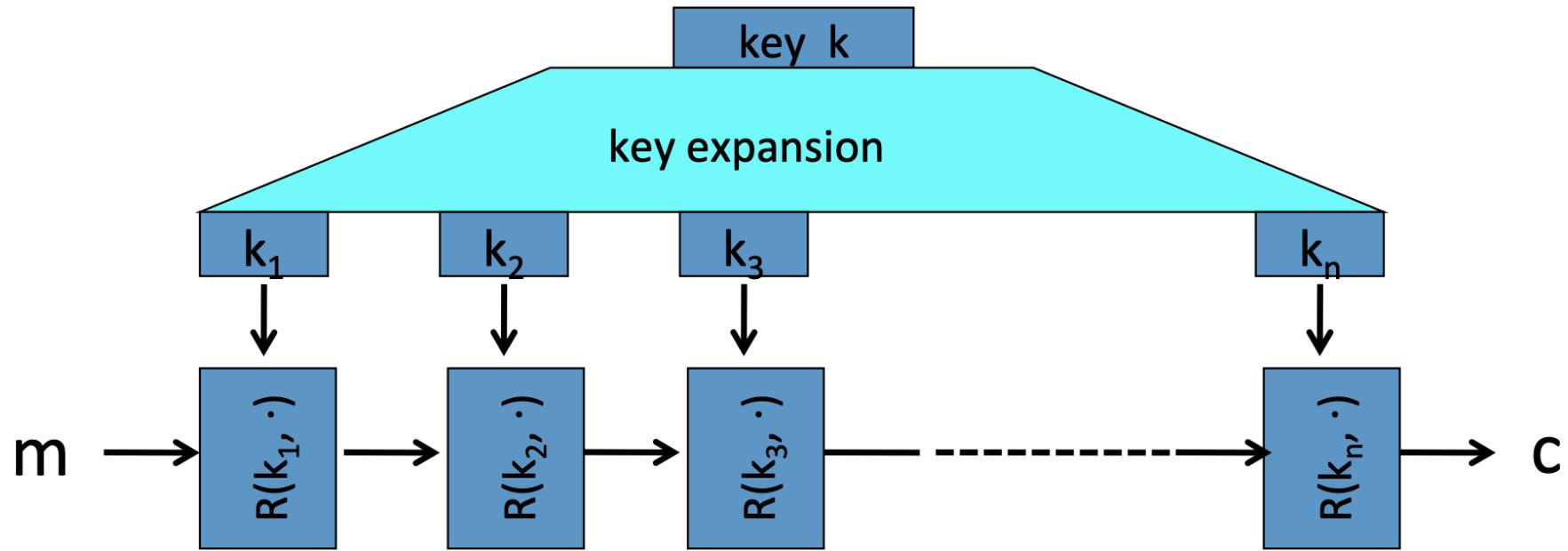
Cifras de Bloco

- Cifras de bloco



- DES: $n = 64$, $k = 56$
- 3DES: $n = 64$, $k = 168$
- AES: $n = 128$, $k = 128, 192, 256$

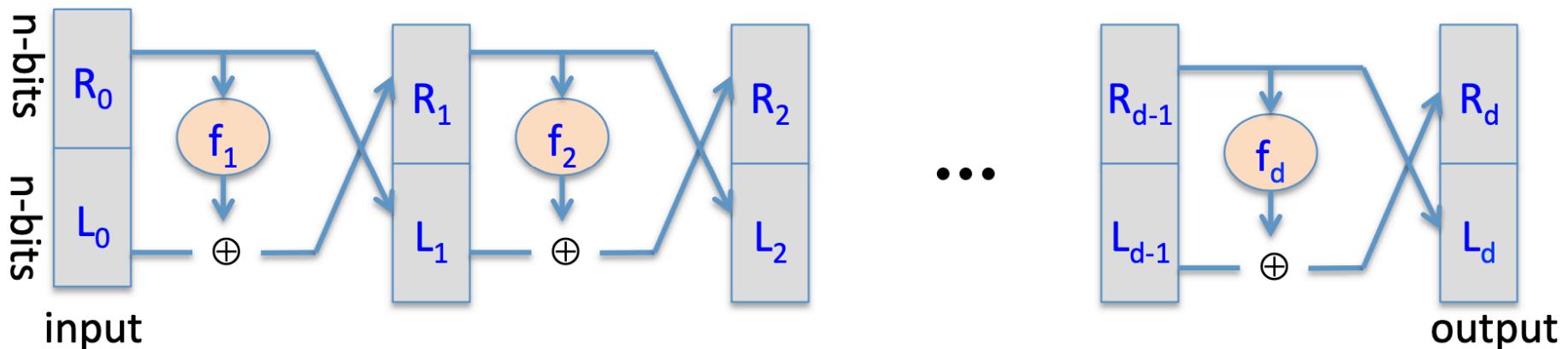
Cifras de Bloco



- $R(k, m)$ é uma round function

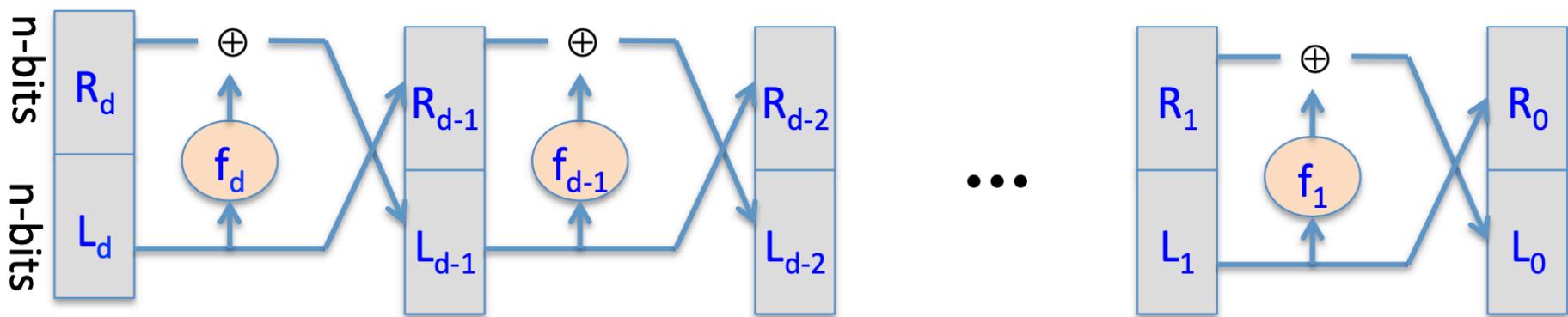
Cifras de Bloco

- Rede de Feistel - encriptação
 - $L_i = R_{i-1}$
 - $R_i = L_{i-1} \oplus F_i(R_{i-1})$



Cifras de Bloco

- Rede de Feistel - decriptação
 - $R_{i-1} = L_i$
 - $L_{i-1} = R_i \wedge F_i(L_i)$

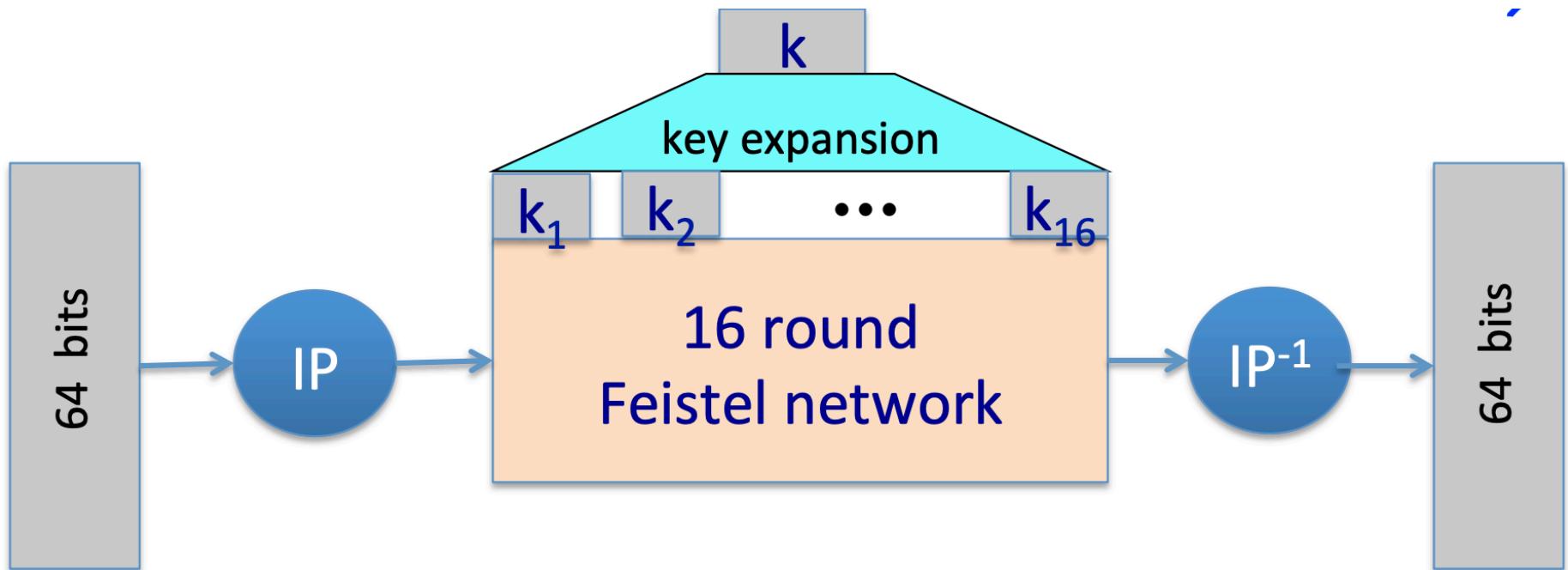


Cifras de Bloco

- DES (1974)
 - Data Encryption Standard
 - 56 bits tamanho da chave
 - 64 bits tamanho do bloco

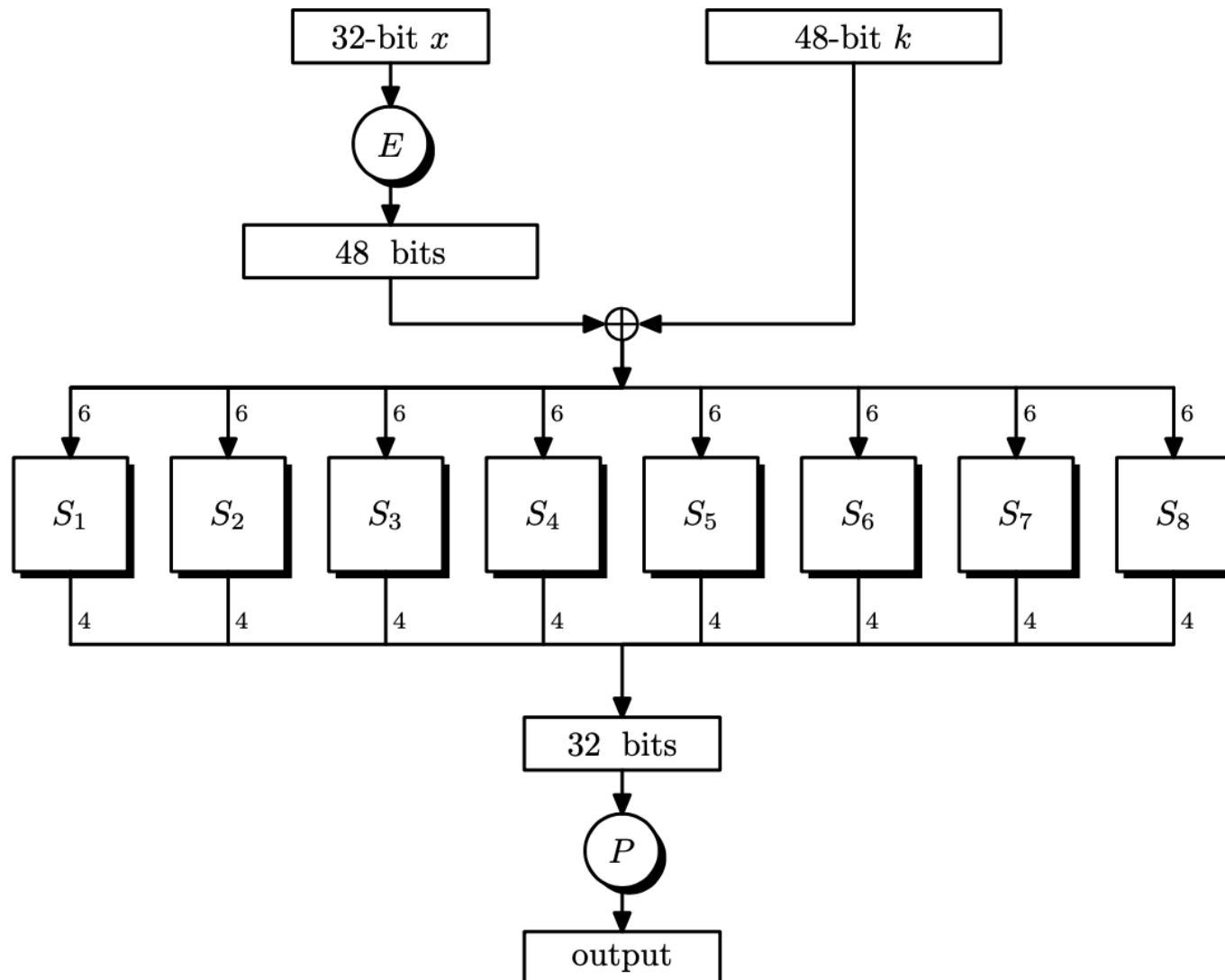
Cifras de Bloco

- DES



Cifras de Bloco

- DES



Cifras de Bloco

- DES

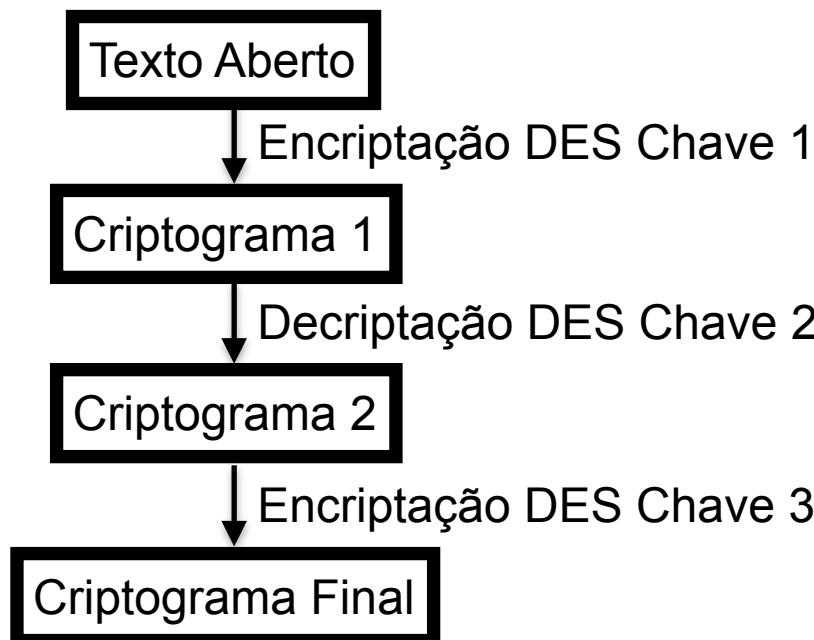
S ₅		Middle 4 bits of input															
		0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
Outer bits	00	0010	1100	0100	0001	0111	1010	1011	0110	1000	0101	0011	1111	1101	0000	1110	1001
	01	1110	1011	0010	1100	0100	0111	1101	0001	0101	0000	1111	1010	0011	1001	1000	0110
	10	0100	0010	0001	1011	1010	1101	0111	1000	1111	1001	1100	0101	0110	0011	0000	1110
	11	1011	1000	1100	0111	0001	1110	0010	1101	0110	1111	0000	1001	1010	0100	0101	0011

Cifras de Bloco

- Criptoanálise
 - Ataques na implementação
 - Ataques lineares
 - Ataques diferenciais
 - Ataques quânticos

Cifras de Bloco

- 3DES
 - Triple Data Encryption Standard
 - 168 bits tamanho da chave
 - 64 bits tamanho do bloco



Cifras de Bloco

- Programa DES

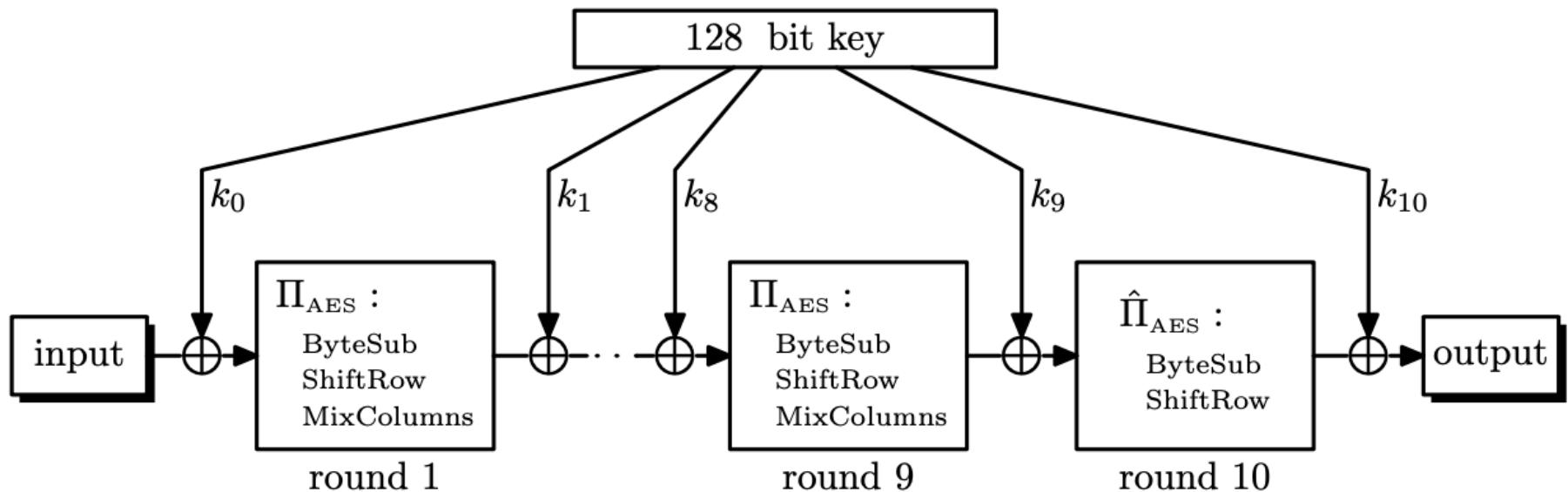
Cifras de Bloco

Cifras de Bloco

- AES (2001)
 - Advanced Encryption Standard
 - 128, 192, 256 bits tamanho da chave
 - 128 bits tamanho do bloco
 - Rijndael, cifra desenvolvida por dois Belgas

Cifras de Bloco

- AES



- Chave 128 bits → 10 rodadas
- Chave 192 bits → 12 rodadas
- Chave 256 bits → 14 rodadas

Cifras de Bloco

- AES
 - Permutação Π
 - Organizar os 128 bits da entrada em uma matriz 4x4 com 8 bits em cada célula
 - Sequência de 3 operações inversíveis
 - ByteSub: permutação codificada de cada célula
 - ShiftRow: deslocamento cíclico das células nas linhas

$$\begin{pmatrix} a_0 & a_1 & a_2 & a_3 \\ a_4 & a_5 & a_6 & a_7 \\ a_8 & a_9 & a_{10} & a_{11} \\ a_{12} & a_{13} & a_{14} & a_{15} \end{pmatrix} \Rightarrow \begin{pmatrix} a_0 & a_1 & a_2 & a_3 \\ a_5 & a_6 & a_7 & a_4 \\ a_{10} & a_{11} & a_8 & a_9 \\ a_{15} & a_{12} & a_{13} & a_{14} \end{pmatrix}$$

- MixColumns: multiplicação de matrizes

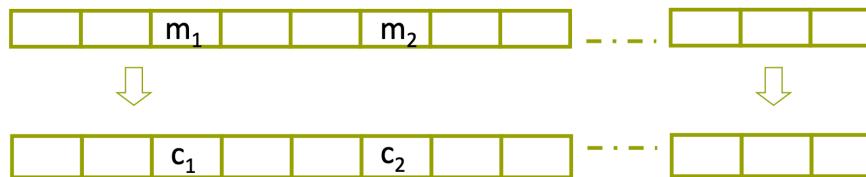
$$\begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \times \begin{pmatrix} a_0 & a_1 & a_2 & a_3 \\ a_5 & a_6 & a_7 & a_4 \\ a_{10} & a_{11} & a_8 & a_9 \\ a_{15} & a_{12} & a_{13} & a_{14} \end{pmatrix} \Rightarrow \begin{pmatrix} a'_0 & a'_1 & a'_2 & a'_3 \\ a'_4 & a'_5 & a'_6 & a'_7 \\ a'_8 & a'_9 & a'_{10} & a'_{11} \\ a'_{12} & a'_{13} & a'_{14} & a'_{15} \end{pmatrix}$$

Cifras de Bloco

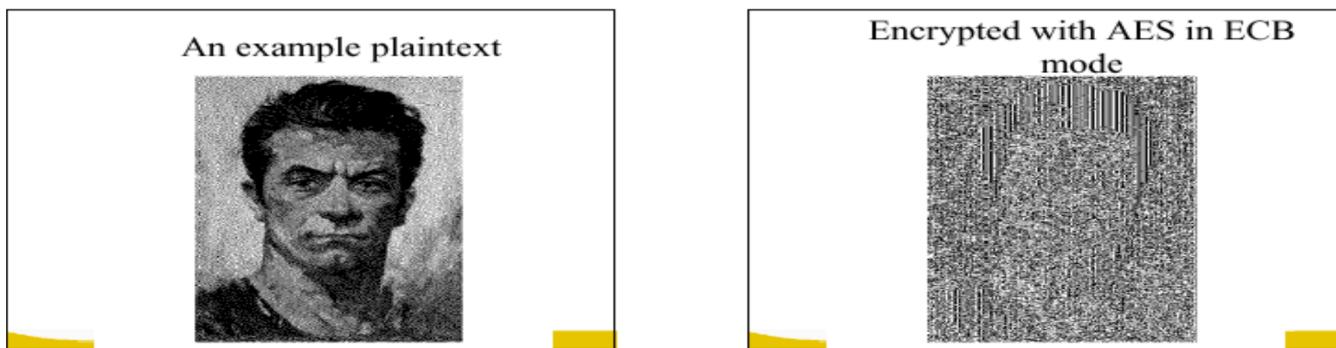
- AES
 - Cifra considerada segura atualmente
 - Tabelas pré calculadas aceleram o processamento
 - Implementação em hardware (Intel Instruction Set)

Cifras de Bloco

- AES
 - Modos de operação
 - Electronic code book (ECB)



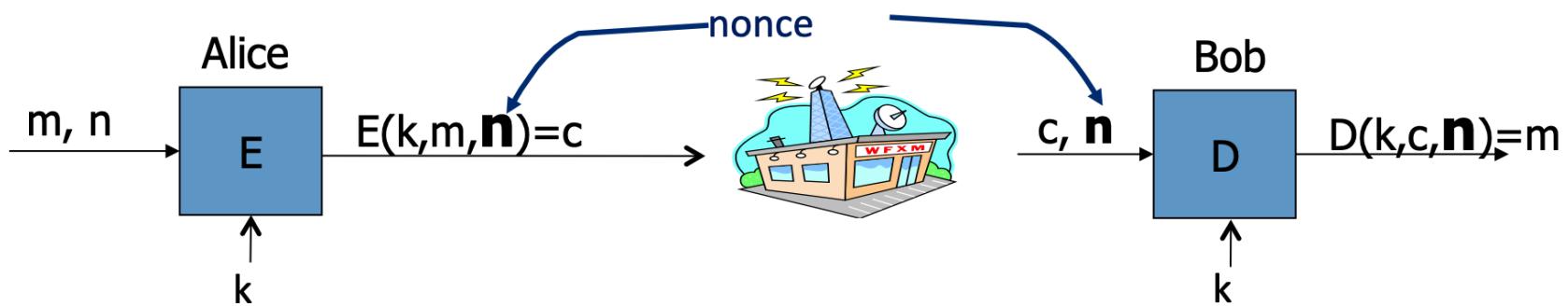
- Se $m_1 == m_2$, então $c_1 == c_2$



- Inseguro (!)

Cifras de Bloco

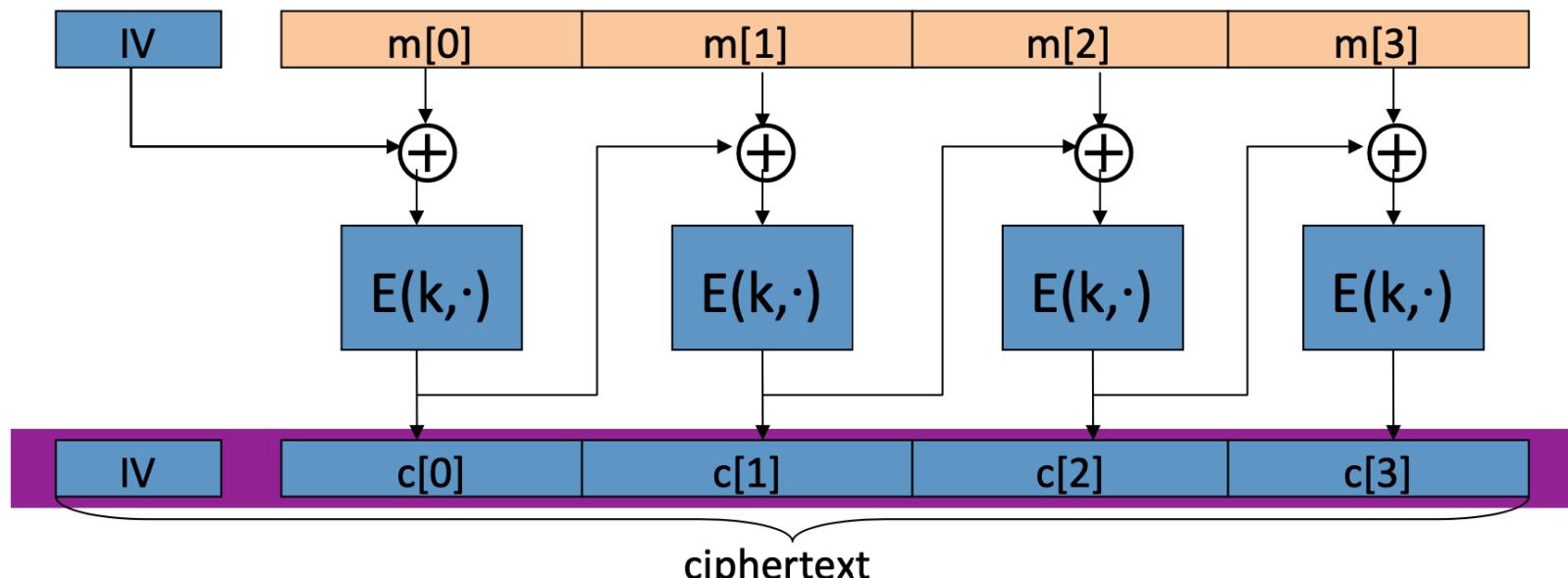
- AES
 - Modos de operação
 - Nonce-based encryption



- Nonce nada mais é do que um contador
- Funciona muito bem para criptografia de rede
- Funciona muito bem para criptografia de arquivos

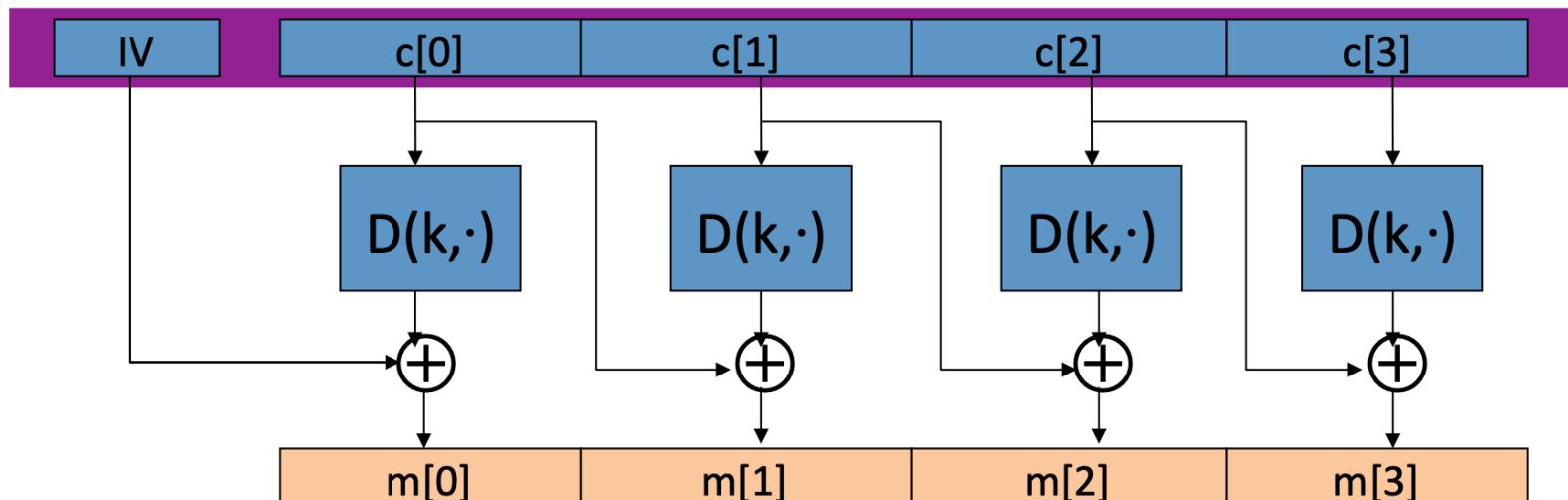
Cifras de Bloco

- AES
 - Modos de operação
 - Cipher block chaining (CBC)
 - Circuito de encriptação



Cifras de Bloco

- AES
 - Modos de operação
 - Cipher block chaining (CBC)
 - Circuito de decriptação

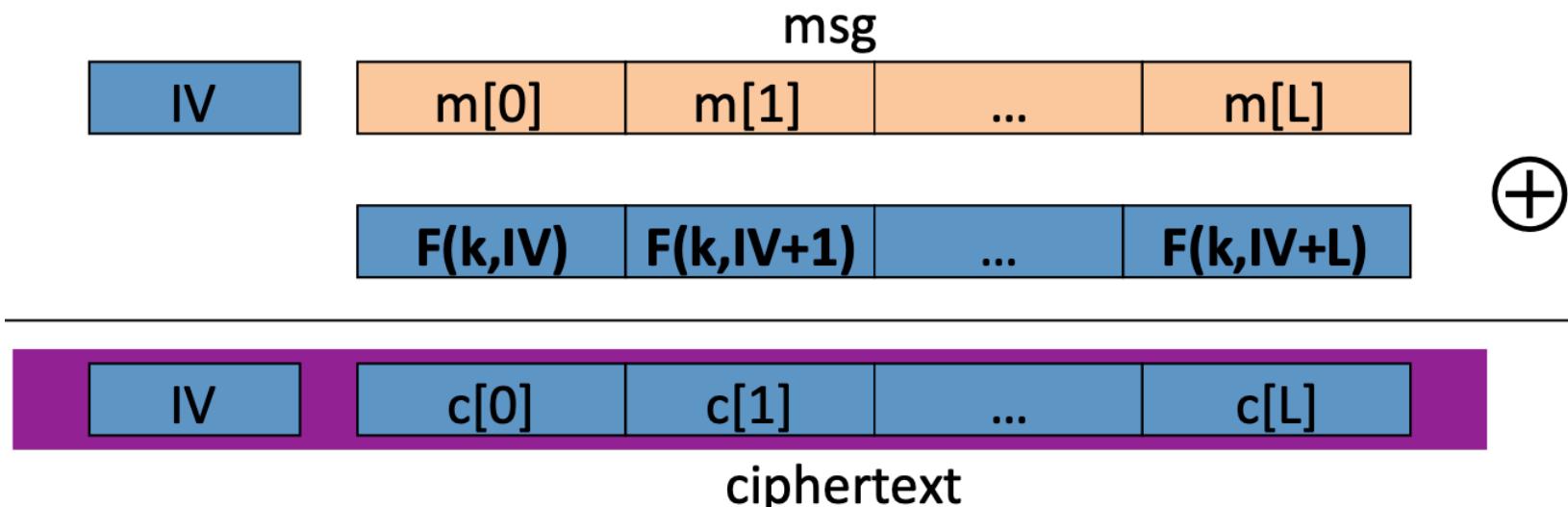


Cifras de Bloco

- AES
 - Modos de operação
 - Cipher block chaining (CBC)
 - $c[0] = E(k, IV \wedge m[0])$
 - $m[0] = D(k, c[0]) \wedge IV$

Cifras de Bloco

- AES
 - Modos de operação
 - Counter (CTR)



Cifras de Bloco

CEUB

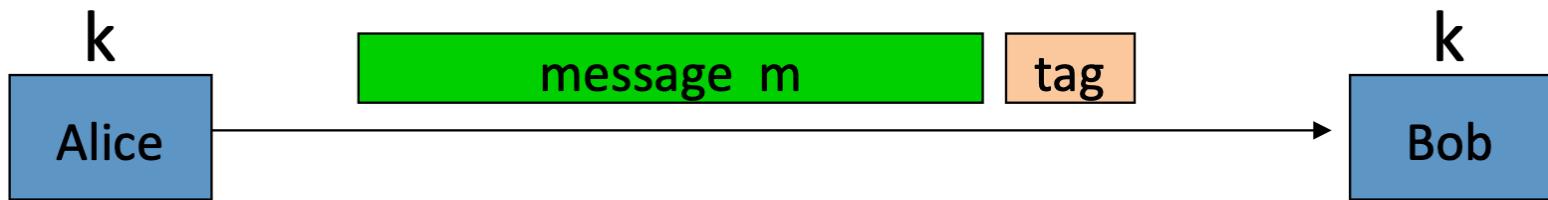
EDUCAÇÃO SUPERIOR

- Programa AES

Garantia de Integridade

Garantia de Integridade

- Definição: Message Authentication Code (MAC)
 - Sejam (S, V) algoritmos definidos sobre (K, M, T)
 - $S(k, m) \rightarrow t$
 - $V(k, m, t) \rightarrow 0, 1$



- Por que a senha é obrigatória, e não apenas um Cyclic Redundancy Check (CRC) ?

Garantia de Integridade

- CBC-MAC
- ECBC-MAC
- CMAC
- NMAC
- PMAC
- Carter-Wegman MAC

Garantia de Integridade

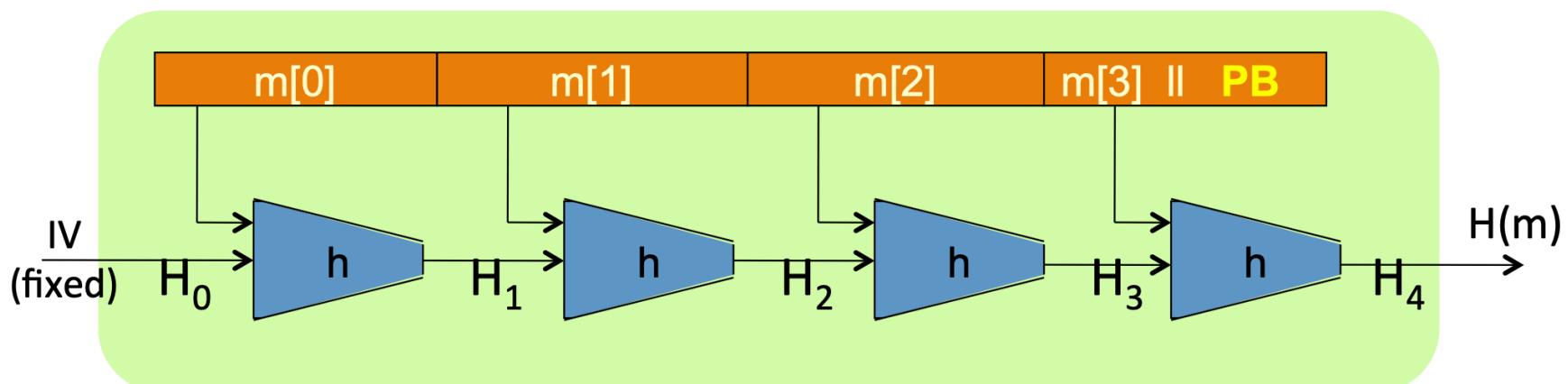
- Definição: resistência à colisão
 - Seja $H:M \rightarrow T$ uma função de resumo ($|M| \gg |T|$)
 - Uma colisão para H é um par $m_0, m_1 \in M$ tal que $H(m_0) == H(m_1)$ e $m_0 != m_1$
 - A função H é resistente à colisão se não houver algoritmo eficiente para encontrar uma colisão

Garantia de Integridade

- Função de compressão de Davis-Meyer
 - Seja (E, D) uma cifra de bloco sobre (K, X) .
 - A função de compressão derivada de E mapeia entradas em $X \times K$ para saídas em X
 - $h(x, k) = E(k, x) \wedge x$

Garantia de Integridade

- Construção iterativa Merkle-Damgard



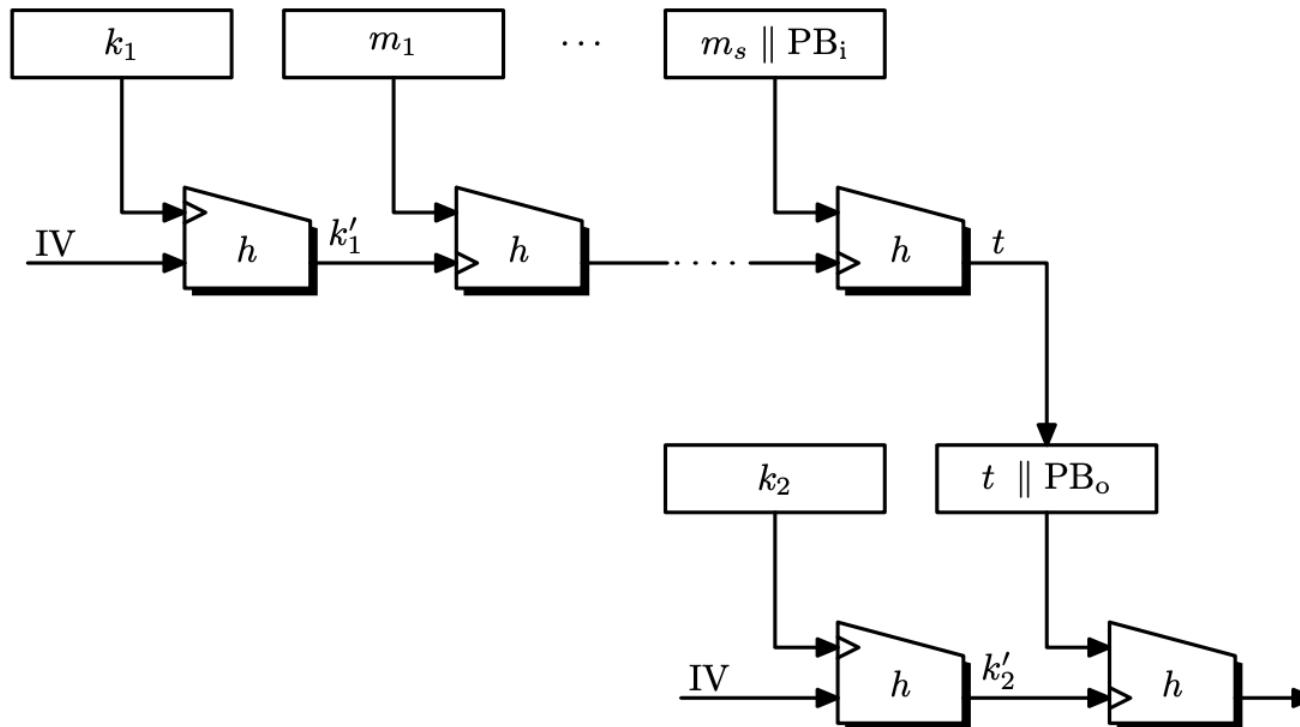
Garantia de Integridade

- SHA-256
 - Davies-Meyer
 - Merkle-Damgard
 - Cifra de bloco SHACAL-2
 - IV = 6A09E667 BB67AE85 3C6EF372 A54FF53A
510E527F 9B05688C 1F83D9AB 5BE0CD19

Garantia de Integridade

- Hash-MAC

- $k_1 = k \wedge \text{ipad}$ (byte 0x36 repetido $|k|$ vezes)
- $k_2 = k \wedge \text{opad}$ (byte 0x5C repetido $|k|$ vezes)



Garantia de Integridade

- Ataque de tempo
 - Submeter mensagem e tag zerada e esperar a resposta (provavelmente negativa)
 - Incrementar o primeiro byte da tag e submeter novamente, medindo o tempo da resposta
 - Quando demorar milesimamente a mais a resposta, significa que o primeiro byte passou, e deu erro no segundo
 - Repetir o processo para cada byte até adivinhar a resposta correta

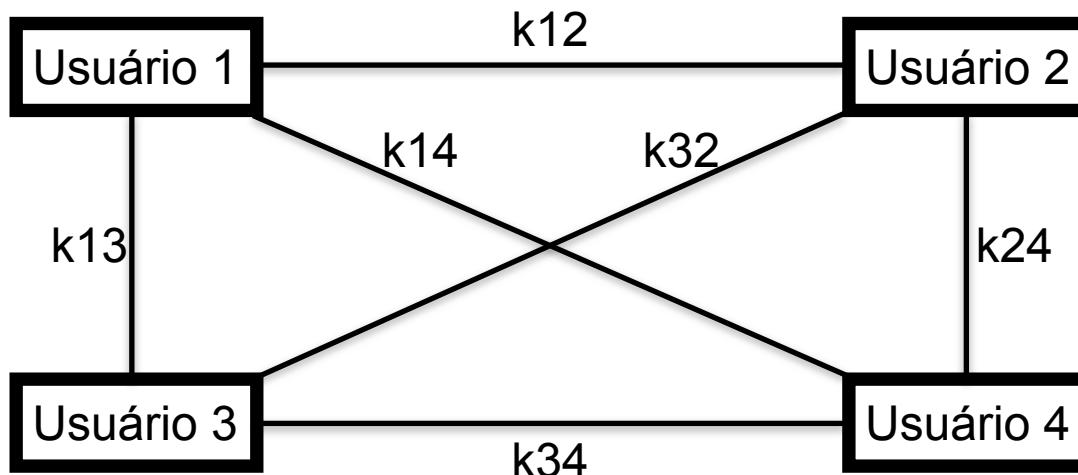
Garantia de Integridade

- Programa SHA-256

Distribuição de Chaves

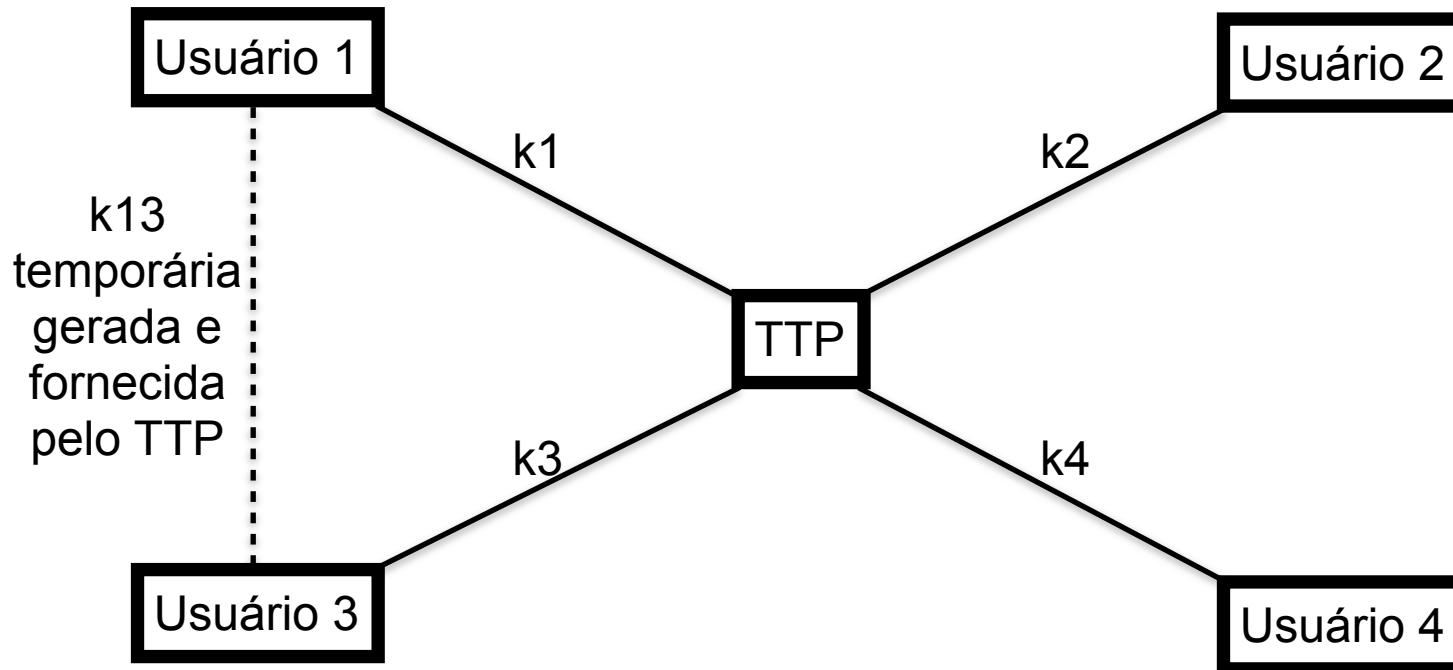
Distribuição de Chaves

- Quando muitos usuários precisam se comunicar seguramente, são necessárias uma chave secreta entre cada um deles, o que é logicamente difícil de gerenciar



Distribuição de Chaves

- Uma solução melhor seria confiar em um terceiro (TTP) em que cada usuário conhecesse apenas uma chave secreta com ele



Distribuição de Chaves

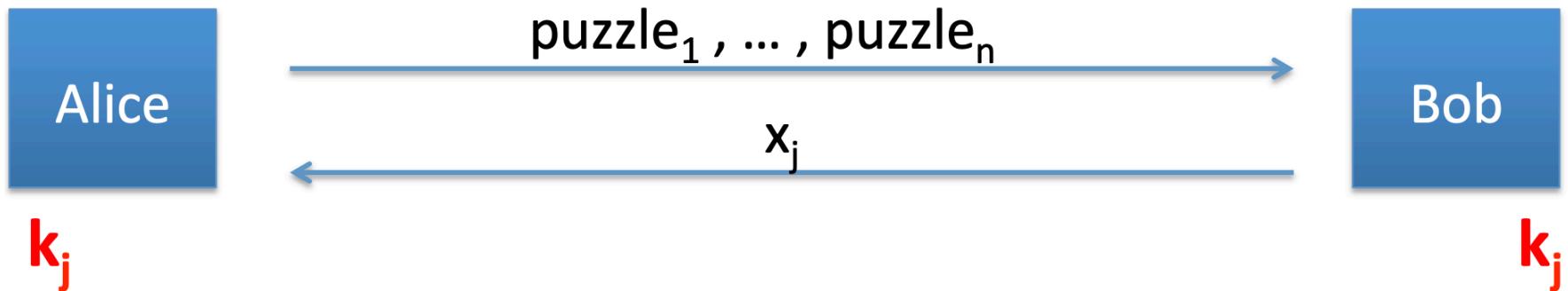
- É possível se livrar do TTP ?
 - Merkle (1974)
 - Diffie-Hellman (1976)

Distribuição de Chaves

- Merkle Puzzles
 - Seja uma cifra simétrica $E(k, m)$ onde $k \in \{0,1\}^{128}$
 - Alice gera todos os 2^{32} enigmas onde a mensagem vai ter um número e uma chave
 - $E(0^{96} \parallel k_1 \dots k_{32}, \text{"Parabéns ! Você quebrou o enigma de número X que tem a chave K"})$
 - Alice envia todos esses enigmas a Bob
 - Bob escolhe um deles aleatoriamente
 - Quebra em 2^{31} tentativas em média (metade do total)
 - Bob devolve X para Alice
 - Ambos usam K como chave compartilhada

Distribuição de Chaves

- Merkle Puzzles



Distribuição de Chaves

- Diffie-Hellman
 - Informações públicas
 - Fixar um número primo p grande (600 dígitos)
 - Fixar um inteiro $g \in \{1, \dots, p\}$
 - Alice escolhe um $a \in \{1, \dots, p - 1\}$
 - Alice calcula $A = g^a \pmod{p}$
 - Bob escolhe um $b \in \{1, \dots, p - 1\}$
 - Bob calcula $B = g^b \pmod{p}$
 - Alice envia A a Bob, Bob envia B a Alice
 - Alice calcula $B^a \pmod{p} \rightarrow g^{b^a} \rightarrow g^{(b*a)}$
 - Bob calcula $A^b \pmod{p} \rightarrow g^{a^b} \rightarrow g^{(a*b)}$

Distribuição de Chaves

- Diffie-Hellman
 - Logaritmo discreto é função difícil de se calcular
 - Fatoração é função difícil de se calcular
 - Gauss (1805): “The problem of distinguishing prime numbers from composite numbers and of resolving the later into their prime factors is known to be one of the most important and useful in arithmetic.”
 - Melhores algoritmos atualmente da ordem de $n^{1/3}$
 - Transição lenta dos algoritmos com base em mod p para as curvas elípticas
 - Ataque do man-in-the-middle (MiTM)

Distribuição de Chaves

- Programa Diffie-Hellman
 - Primo p
 - 102031405123416071809152453627382938465749
676859789
 - Base g
 - 1234567890123456789012345

Criptografia Assimétrica

Criptografia Assimétrica

- Definição: cifra assimétrica
 - Seja um conjunto K
 - Seja um conjunto M
 - Seja um conjunto C
 - Seja uma tripla de algoritmos eficientes G, E, e D, tais que
 - $G()$: algoritmo não determinístico que gera um par de chaves (pk, sk)
 - $E(pk, m)$: algoritmo não determinístico que recebe $m \in M$ e gera $c \in C$
 - $D(sk, c)$: algoritmo determinístico que recebe $c \in C$ e gera $m \in M$
 - Consistência: $\forall(pk, sk) \text{ gerados por } G$
 - $\forall m \in M: D(sk, E(pk, m)) == m$

Criptografia Assimétrica

- Definição: trapdoor function (TDF)
 - Seja um conjunto X
 - Seja um conjunto Y
 - Seja uma tripla de algoritmos eficientes G, F, e F-1, tais que
 - G(): algoritmo não determinístico que gera um par de chaves (pk, sk)
 - F(pk, x): algoritmo determinístico que define uma função $X \rightarrow Y$
 - F-1(sk, y): algoritmo determinístico que define uma função $Y \rightarrow X$ que inverte F(pk, x)
 - Consistência: $\forall(pk, sk) \text{ gerados por } G$
 - $\forall x \in X: F^{-1}(sk, F(pk, x)) == x$

Criptografia Assimétrica

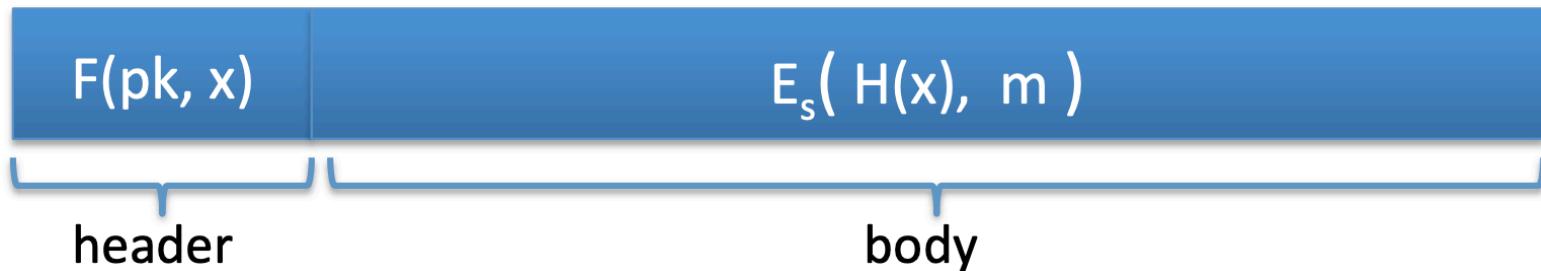
- Criptografia de chave pública usando TDF
 - Nunca criptografar a mensagem diretamente (!)
 - $c = F(pk, m)$
 - $m = F^{-1}(sk, c)$
 - Como é determinístico, é vulnerável a muitos ataques (!)

Criptografia Assimétrica

- Criptografia de chave pública usando TDF
 - Sejam os algoritmos (G, F, F^{-1}) uma TDF $X \rightarrow Y$
 - Sejam (E, D) uma cifra simétrica
 - Seja $H: X \rightarrow K$ uma função de hash
 - $E(pk, m)$
 - $\forall x \in X$
 - $y = F(pk, x) \quad k = H(x) \quad c = E(k, m)$
 - retorna (y, c)
 - $D(sk, (y, c))$
 - $x = F^{-1}(sk, y) \quad k = H(x) \quad m = D(k, c)$
 - retorna m

Criptografia Assimétrica

- Criptografia de chave pública usando TDF



Criptografia Assimétrica

- RSA (1977)
 - Ronald Rivest, Adi Shamir, and Leonard Adleman
 - SSL, TLS
 - Criptografia de e-mail
 - Criptografia de sistema de arquivos
 - HTTPS
 - ...

Criptografia Assimétrica

- RSA
 - Geração das chaves
 - Escolher de forma aleatória dois números primos grandes p e q
 - Calcular $n = p * q$
 - $Z_n = \{0, 1, 2, \dots, n-1\}$
 - $(Z_n)^* = \{\text{elementos inversíveis em } Z_n\}$
 - Calcular a função Função φ de Euler em n
 - $\varphi(n) = (p - 1) * (q - 1)$
 - $\varphi(n) = n - p - q + 1$
 - A quantidade de elementos do conjunto $(Z_n)^* == \varphi(n)$

Criptografia Assimétrica

- RSA
 - Geração das chaves
 - Teorema de Euler
 - $\forall x \in (\mathbb{Z}_n)^*: x^{\varphi(n)} \equiv 1$
 - Escolher um inteiro e tal que $1 < e < \varphi(n)$
 - Calcular d de forma que $d * e \equiv 1 \pmod{\varphi(n)}$, ou seja, d seja o inverso multiplicativo de e em mod $\varphi(n)$
 - pk: (n, e)
 - sk: (n, d)

Criptografia Assimétrica

CEUB

EDUCAÇÃO SUPERIOR

- RSA
 - Operação
 - $c = m^e \pmod{n}$
 - $m = c^d \pmod{n}$
 - Nunca criptografar a mensagem diretamente (!)
 - Como é determinístico, é vulnerável a muitos ataques (!)

Criptografia Assimétrica

- Criptografia de chave pública usando RSA
 - Quanto menor o e, mais rápido o algoritmo executa
 - Valor recomendado: $e == 65537 == 2^{16}+1$

Criptografia Assimétrica

- Programa RSA simplificado para demonstração

Criptografia Assimétrica

Criptografia Assimétrica

- Criptografia de chave pública usando RSA
 - Seja o algoritmo G tal que gere as chaves do RSA
 - $pk(n, e)$
 - $sk(n, d)$
 - Sejam (E, D) uma cifra simétrica
 - Seja $H: Z_n \rightarrow K$ uma função de hash
 - $E(pk, m)$
 - $\forall x \in Z_n$
 - $y = RSA(pk, x) \quad k = H(x) \quad c = E(k, m)$
 - retorna (y, c)
 - $D(sk, (y, c))$
 - $x = RSA^{-1}(sk, y) \quad k = H(x) \quad m = D(k, c)$
 - retorna m

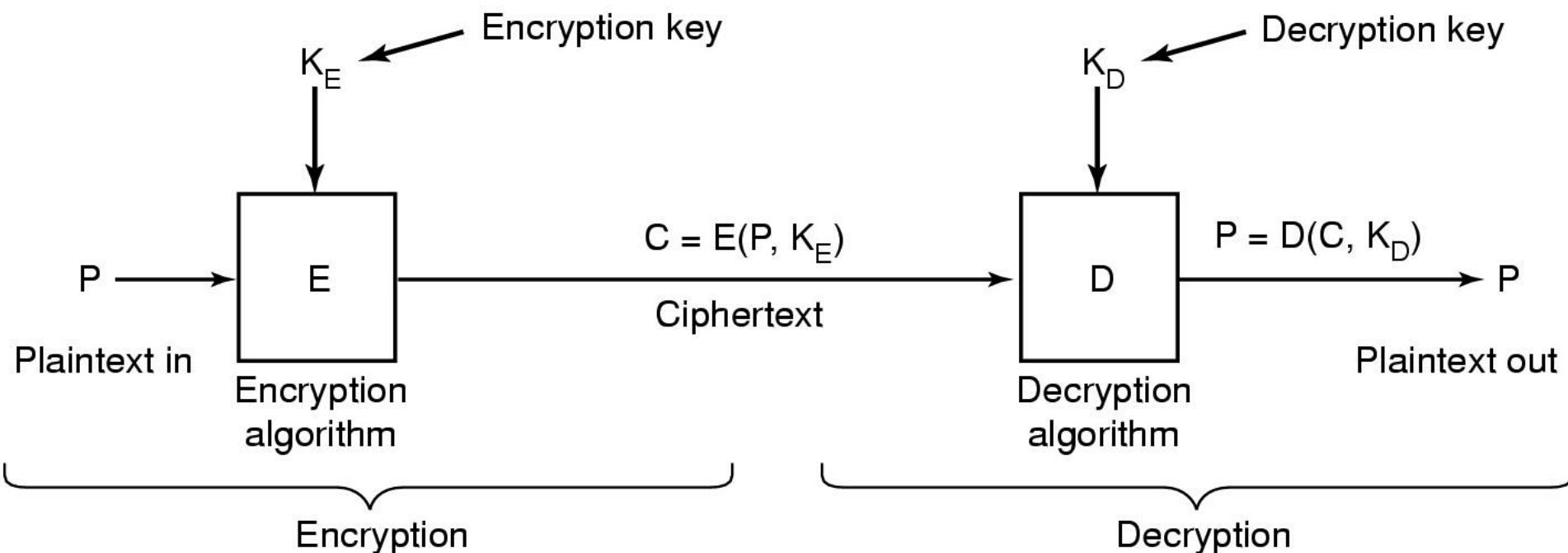
Criptografia Assimétrica

- Programa RSA como deve ser feito

Criptografia Assimétrica

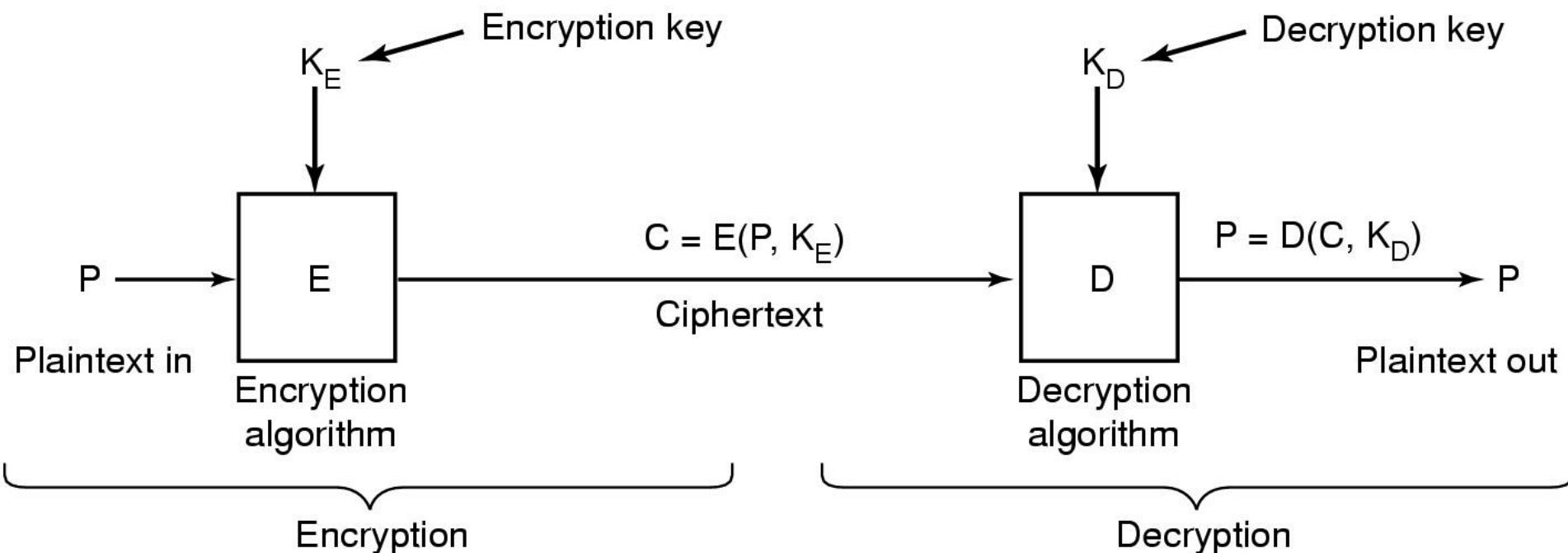
Criptografia Assimétrica

- Criptografia assimétrica para sigilo
 - Criptografar usando a chave pública do destinatário



Criptografia Assimétrica

- Criptografia assimétrica para autenticação
 - Criptografar usando a chave secreta do remetente



Criptografia Assimétrica

- Criptografia assimétrica para sigilo e autenticação
 - Criptografar usando a chave pública do destinatário, somado à chave secreta do remetente
 - Remetente
 - $E(pkDest, m) \rightarrow c$
 - $E(skRem, c) \rightarrow a$
 - Envia (c, a)
 - Destinatário
 - $D(pkRem, a) \rightarrow c$
 - $D(skDest, c) \rightarrow m$

Criptografia Assimétrica

- Assinatura digital
 - Autoridade certificadora (CA)
 - Certificados X.509
 - Cadeia de certificados
 - Token criptográfico
 - Autenticação segura na Internet
 - Legislação
 - Senha SEI (?!?)

Criptografia Assimétrica

- Programa assinatura digital

Segurança de Sistemas

Segurança de Sistemas

CEUB

EDUCAÇÃO SUPERIOR

- Ameaças
- Risco
- Grau de dano
- Medidas defensivas

- Ameaças a usuários
 - Roubo de identidade
 - Shoulder surfing
 - Garbage diving
 - Engenharia social
 - Métodos de alta tecnologia
 - Perda de privacidade
 - Registros públicos na Internet
 - Monitoramento, perfilamento e espionagem na Internet

- Ameaças a usuários
 - Ferramentas de espionagem on-line
 - Cookies
 - Web bugs
 - Spyware
 - Spam
 - Ferimento relacionado ao uso de computadores
 - Ergonomia

- Ameaças ao hardware
 - Ameaças relacionadas a energia
 - Flutuação na rede
 - DDoS – Distributed denial of service
 - Roubo e vandalismo
 - Desastres naturais

- Ameaças aos dados
 - Vírus
 - Hacking
 - Sniffing
 - Spoofing
 - Intrusion
 - Cyber terrorismo
 - Botnet
 - Ransomware

- Proteção dos usuários
 - Gerenciar seus papéis
 - Guardar informações pessoais
 - Atenção ao preencher formulários
 - Conhecer seus direitos
 - Gerenciar cookies
 - Remover web bugs e spywares
 - Fugir de spams

- Proteção do hardware
 - Avisos de eventos automáticos
 - Sala cofre
 - Magnetismo
 - Temperatura
 - Humidade
 - Poeira

- Proteção dos dados
 - Limitar acesso físico
 - Firewall
 - Backup

- Estratégias de segurança
 - Menor privilégio necessário
 - Defesa em profundidade
 - Múltiplas camadas de defesa
 - Gargalo
 - Concentração do tráfego facilita o monitoramento
 - Link mais fraco da corrente
 - Fail-safe stance
 - O sistema, ao notar um erro, trava o acesso a todos

- Estratégias de segurança
 - Default deny stance
 - Tudo que não for expressamente permitido é proibido
 - Default permit stance
 - Tudo que não for expressamente proibido é permitido
 - Participação universal
 - Diversidade dos tipos de defesa
 - Simplicidade

Protocolos de Autenticação

Protocolos de Autenticação

CEUB

EDUCAÇÃO SUPERIOR

- Aplicações
 - Abrir uma fechadura
 - Destrarvar um veículo
 - Login em um ATM bancário
 - Login online em uma conta bancária

Protocolos de Autenticação

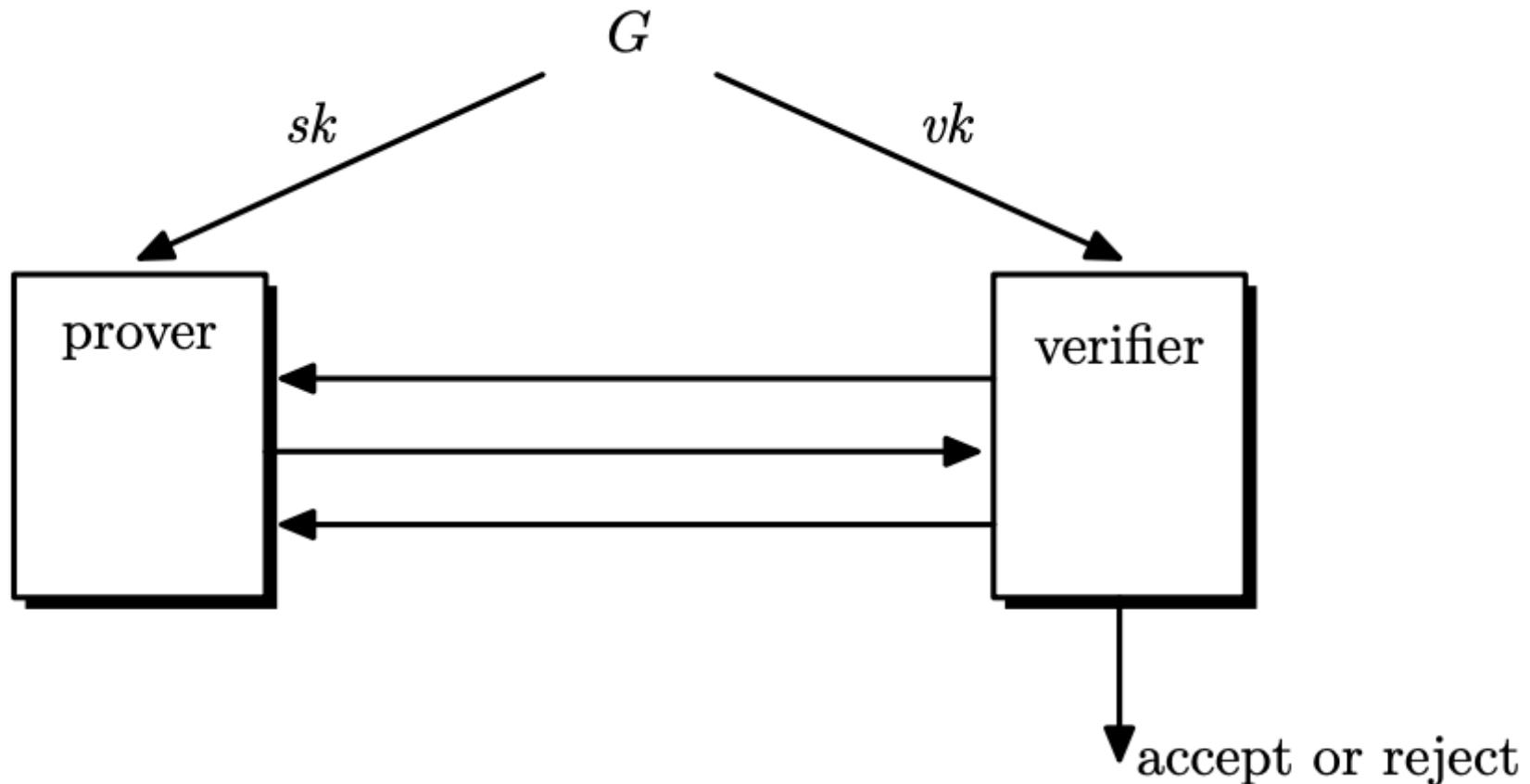
CEUB

EDUCAÇÃO SUPERIOR

- Protocolos de identificação
 - Um provador tem uma chave secreta sk e a utiliza para convencer um verificador de sua identidade
 - Um verificador tem uma chave de verificação vk e a utiliza para confirmar a solicitação do provador

Protocolos de Autenticação

- Protocolos de identificação



Protocolos de Autenticação

CEUB

EDUCAÇÃO SUPERIOR

- Ataques
 - Direto
 - Senha protege
 - Eavesdropping
 - Senha de uso único protege
 - Ativos
 - Challenge-response protege

Protocolos de Autenticação

CEUB

EDUCAÇÃO SUPERIOR

- Chaves de verificação
 - Públicas
 - Secretas
- Protocolos
 - Stateless
 - sk e vk são eternamente perenes
 - Stateful
 - sk e vk são atualizadas recorrentemente

- Protocolo de senha
 - Segurança contra ataque direto
 - Hashes das senhas armazenadas nos servidores de autenticação
 - c:\windows\system32\password (!?)
 - /etc/passwd (!?)
 - /etc/shadow (!?)

Protocolos de Autenticação

- Crack de senhas por meio de ataque de dicionário
 - 15 senhas mais comuns vazadas a partir de 5 milhões de casos nos EUA e Europa Ocidental
 - 123456, password, 12345, 12345678, football, qwerty, 1234567890, 1234567, princess, 1234, login, welcome, solo, abc123, admin

Protocolos de Autenticação

CEUB

EDUCAÇÃO SUPERIOR

- Ataque de dicionário online
 - Aumento proposital do tempo de resposta do servidor frente a tentativas de senhas incorretas
 - Atacante fixa a senha e força variação do usuário com spoofing de IP

Protocolos de Autenticação

- Ataque de dicionário offline
 - Invasão e recuperação do arquivo de senhas
 - CrackStation disponibiliza um dicionário com 1.5 bilhão de senhas
 - Evidências empíricas sugerem que 50% das senhas “normais” criadas por pessoas estão nesse dicionário
 - Ora, se forem testados 1.5 bilhão de senhas, portanto, 1 ou 2 serão encontradas
 - Se o hash for o SHA-256, padrão, gastam-se minutos em uma GPU de mercado
 - Pré-processamento reduz o tempo do ataque significativamente

Protocolos de Autenticação

CEUB

EDUCAÇÃO SUPERIOR

- Dificultando o ataque de dicionário
 - Salt público (salt)
 - String randômica definida para cada nova senha, acrescentada no arquivo de senhas
 - salt, Hash(senha + salt)
 - Salt secreto (pepper)
 - String randômica definida para cada nova senha, acrescentada na senha
 - Hash (senha + pepper)

Protocolos de Autenticação

CEUB

EDUCAÇÃO SUPERIOR

- Dificultando o ataque de dicionário
 - Funções de hash lentas
 - $H(H(H(H(H(H(H(H(senha))))))))$
 - Password-based key derivation function (PBKDF)
 - Slow memory-hard hash functions
 - Password oblivious memory-hard functions

Protocolos de Autenticação

CEUB

EDUCAÇÃO SUPERIOR

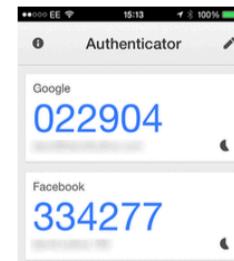
- Problema mais sério de todos (!)
 - Uso da mesma senha em vários serviços diferentes
 - Servidores bem implementados, protegidos com salt ou hash lento, ainda assim podem ser invadidos por ataques fáceis em servidores mal implementados
 - Biometria resolve (?!?)
 - Biometria não é necessariamente secreta
 - Biometria não é revogável, ao contrário da senha

Protocolos de Autenticação

- Protocolo de senha de uso único
 - Hash-based one-time password (HOTP)
 - Não é seguro
 - Time-based one-time passwords (TOTP)
 - Modelo preferido



(a) RSA SecurID token



(b) Google authenticator

Protocolos de Autenticação

CEUB

EDUCAÇÃO SUPERIOR

- Protocolo de challenge-response
 - Protege o provador de um verificador malicioso
 - Ambos provador e verificador precisam acordar o protocolo de reconhecimento
 - 3DES
 - AES

Protocolos de Autenticação

- Programa crack de senhas

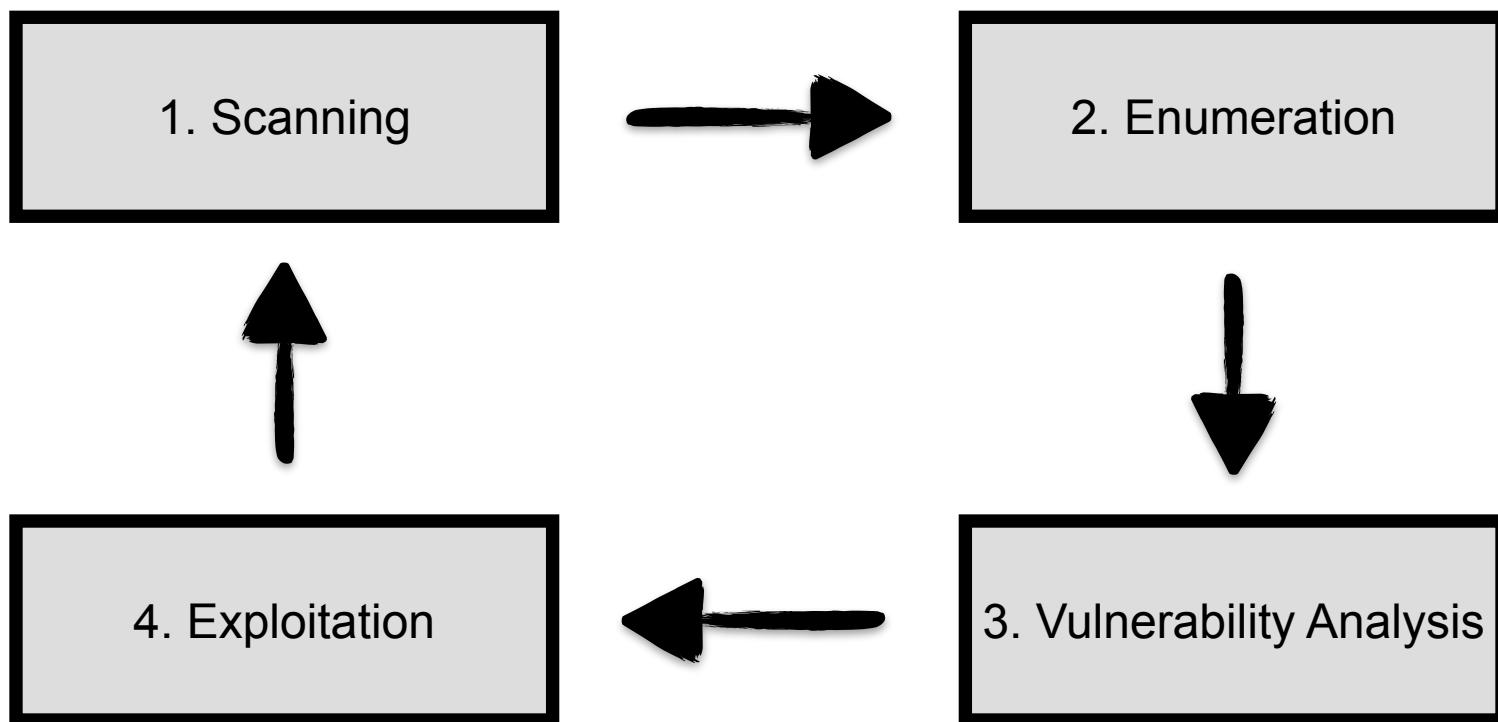
```
root::!:18681:0:99999:7:::  
daemon:*:18681:0:99999:7:::  
bin:*:18681:0:99999:7:::  
sys:*:18681:0:99999:7:::  
sync:*:18681:0:99999:7:::  
man:*:18681:0:99999:7:::  
lp:*:18681:0:99999:7:::  
mail:*:18681:0:99999:7:::  
news:*:18681:0:99999:7:::  
uucp:*:18681:0:99999:7:::  
proxy:*:18681:0:99999:7:::  
www-data:*:18681:0:99999:7:::  
backup:*:18681:0:99999:7:::  
systemd-timesync:*:18681:0:99999:7:::  
systemd-network:*:18681:0:99999:7:::  
systemd-resolve:*:18681:0:99999:7:::  
mysql!:18681:0:99999:7:::  
ntp:*:18681:0:99999:7:::  
_rpc:*:18681:0:99999:7:::  
usbmux:*:18681:0:99999:7:::  
tcpdump:*:18681:0:99999:7:::  
sshd:*:18681:0:99999:7:::  
statd:*:18681:0:99999:7:::  
sshl!:18681:0:99999:7:::  
nm-openvpn:*:18681:0:99999:7:::  
kali:fc5669b52ce4e283ad1d5d182de88fffaec6672bace84ac2ce4c083f54fe2bc:18681:0:99999:7:::  
junior:353b31cbc5fe9caf53063936395072f9369076a7d0c8ee534f834cb2693dd6e2:18681:0:99999:7:::  
mane:8d969eef6ecad3c29a3a629280e686fc0f3f5d5a86aff3ca12020c923adc6c92:18681:0:99999:7:::  
fulano:d58d736c7a967fb5f307951932734fb0594725faa5011dbb66a8c538e635fb6:18681:0:99999:7:::  
beltrano:b7e94be513e96e8c45cd23d162275e5a12ebde9100a425c4ebcd7fa4dc897c:18681:0:99999:7:::  
cicrano:280d44ab1e9f79b5cce2dd4f58f5fe91f0fbacdacf7447dffcc318ceb79f2d02:18681:0:99999:7:::  
gabriel:0c08a9536b5dd78713f440acb930872fd69f7a71da0cf9cdedc9628ddf9ac3d7:18681:0:99999:7:::  
joao:65e84be35332fb784c48129675f9eff3a682b27168c0ea744b2cf58ee02337c5:18681:0:99999:7:::  
humberto:26df939ee38cc162bb98f4eb5a111fdb270db6bd1dc645e98871ac2d8449bd6c:18681:0:99999:7:::  
maria:d04a0747e946c6233ab5a91ceb3a59624cdf14d7fd05e9386d22580ec980455e:18681:0:99999:7:::  
fernanda:756356fbfa52ca1d11812575fc9238edb0cecd44785f2c73d4604c56954d0af:18681:0:99999:7:::  
mario:8c6976e5b5410415bde908bd4dee15dfb167a9c873fc4bb8a81ff2ab448a918:18681:0:99999:7:::  
sunda:d75d2785d90cab90245dc9e22a82c1a048673c4a2c54fa1754e9085f4f01d687:18681:0:99999:7:::  
zulu:e79c15d596b9b9c1334150622ce1ecb016c61e2bf05b7864296a29f9e62ed863:18681:0:99999:7:::  
systemd-coredump:!*:18681:::::
```

Segurança de Sistemas

- Penetration test
- Pentest
- Ethical hacking
- Open Web Application Security Project (OWASP)
 - Mark Curphey 09/09/2001
 - Mutillidae

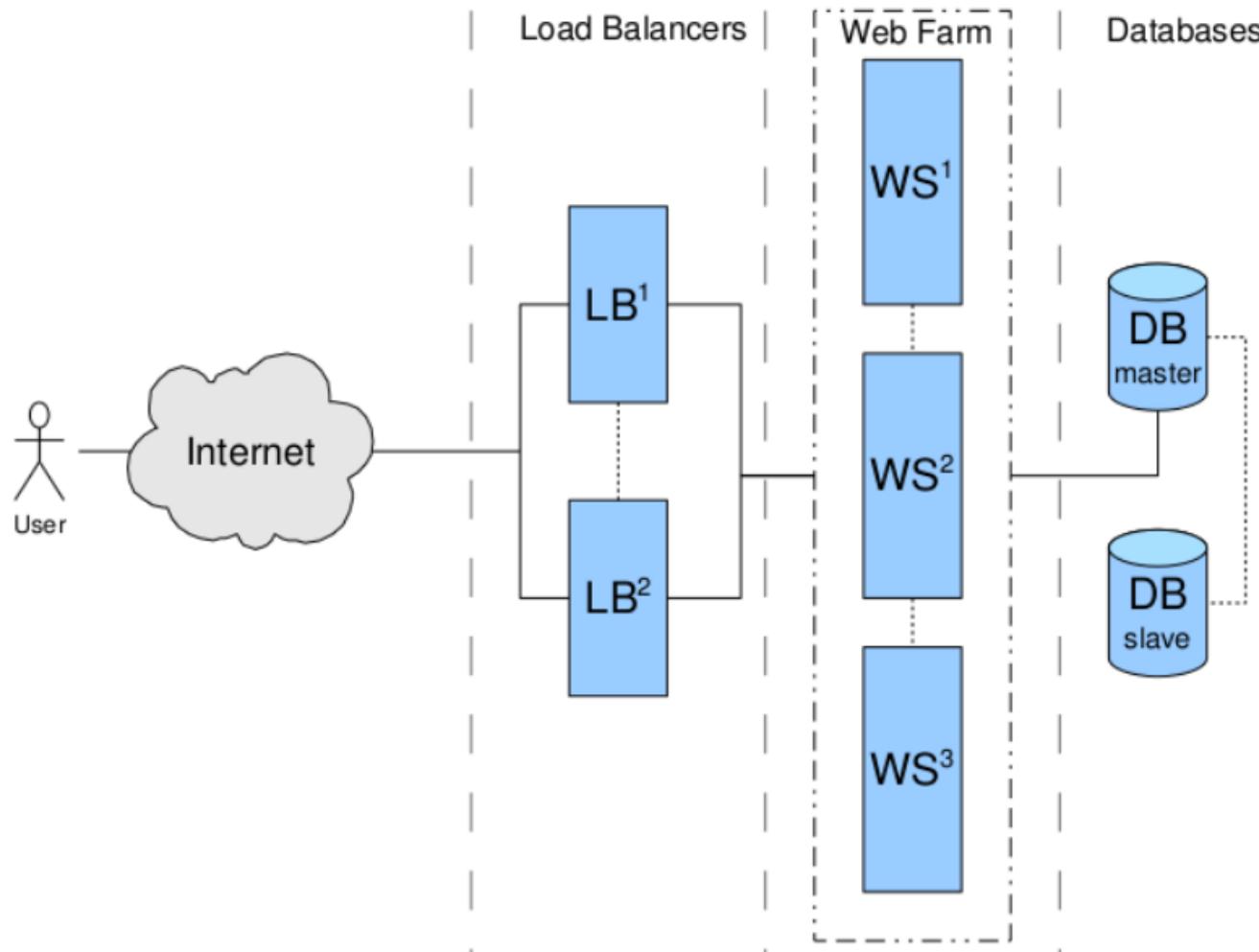
Segurança de Sistemas

- Fases de um ataque

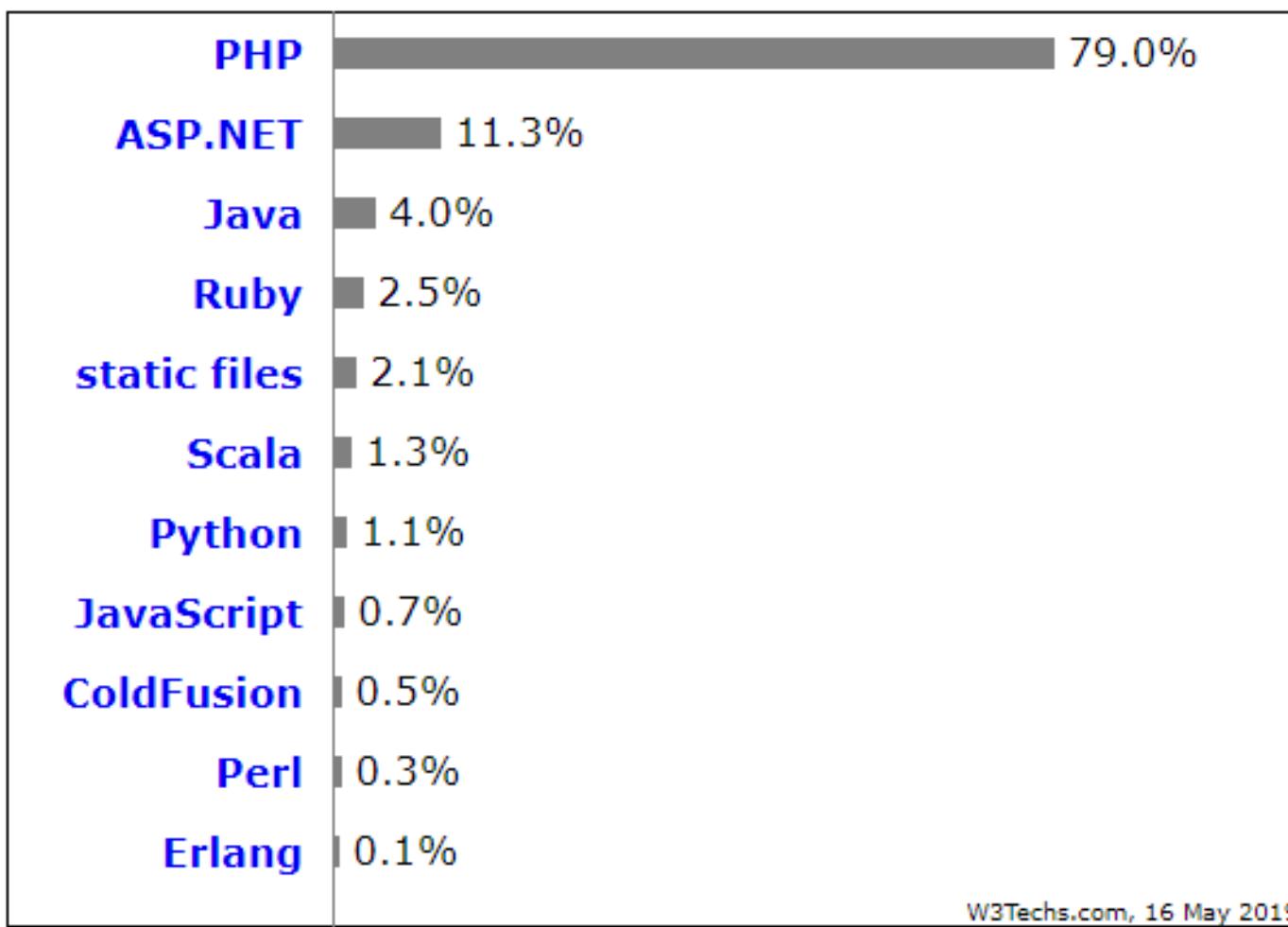


Segurança de Sistemas

- Arquitetura Web



- Arquitetura Web



- Preparação do Ambiente
 - Oracle Virtual Box
 - <https://www.virtualbox.org>
 - Kali Linux
 - <https://www.kali.org>
 - Ubuntu Linux
 - <https://www.ubuntu.com>

- Preparação do Ambiente
 - Criar uma máquina virtual Linux
 - Configurar
 - (1/2) processadores
 - (1/4) GB RAM
 - Placa de rede em modo bridge
 - Instalar o Ubuntu
 - Aumentar a resolução da tela
 - Botão direito do mouse mouse no desktop → Display Setting → Resolution 1920x1440
 - Instalar o VirtualBox Guest Additions
 - Devices → Insert Guest Additions CD Image

- Preparação do Ambiente
 - Instalar o Apache Web Server
 - sudo apt-get update
 - sudo apt-get install apache2
 - sudo a2enmod rewrite
 - sudo systemctl restart apache2
 - sudo vi /etc/apache2/apache2.conf
 - <Directory /var/www/>
 - » AllowOverride All
 - sudo systemctl restart apache2

- Preparação do Ambiente
 - Instalar o PHP
 - sudo apt-get update
 - sudo apt-get install php
 - sudo apt-get install libapache2-mod-php
 - sudo apt-get install php7.4-curl
 - sudo apt-get install php7.4-mbstring
 - sudo apt-get install php7.4-xml
 - sudo vi /var/www/html/index.php
 - <?php echo “Hello World !”; ?>

- Preparação do Ambiente
 - Instalar o MySQL
 - sudo apt-get update
 - cd Downloads
 - sudo wget https://dev.mysql.com/get/mysql-apt-config_0.8.12-1_all.deb
 - sudo dpkg -i mysql-apt-config_0.8.12-1_all.deb
 - ubuntu bionic
 - MySQL Server & Cluster
 - mysql-5.7

- Preparação do Ambiente
 - Instalar o MySQL
 - sudo apt-get update
 - sudo apt-cache policy mysql-server
 - Version table: *5.7.34-1ubuntu18.04*
 - sudo apt-get install mysql-client=**
 - sudo apt-get install mysql-community-server=**
 - Senha do root: mutillidae
 - sudo apt-get install mysql-server=**
 - sudo apt-get install php-mysql

- Preparação do Ambiente
 - Instalar o Git
 - sudo apt-get update
 - sudo apt-get install git

- Preparação do Ambiente
 - Instalar o Mutillidae
 - cd /var/www/html/
 - sudo git clone https://github.com/webpwnized/mutillidae.git mutillidae
 - Reboot
 - http://localhost/mutillidae
 - Reset DB

Segurança de Sistemas

- SQL injection
 - Mutillidae user info
 - Kali sqlmap
 - `http://testphp.vulnweb.com/listproducts.php?cat=1`
 - `sqlmap -u "http://testphp.vulnweb.com/listproducts.php?cat=1" -f -b --dbs`

- Remote command execution
 - Detectar o sistema operacional
 - Concatenador de comandos
 - &
 - |
 - Mutillidae DNS lookup
 - ifconfig
 - nc

- Cross site scripting
 - Mutillidae echo message
 - <script>alert('XSS');</script>
 - <script>alert('Cookies que não têm o atributo
HTTPOnly definido: ' + document.cookie);</script>

- Cross site request forgery
 - Suponha
 - `http://www.bancomalfeito.com.br/transferFunds?amount=1000&destinationAccount=432938741`
 - Crie um site com uma imagem
 - ``
 - Aplique ataque de phishing para esse site
 - Clique aqui para aumentar o tamanho daquilo...

Segurança de Redes

- Modelo Open System Interconnection (OSI)

Aplicação	Processos de rede para aplicação
Apresentação	Representação dos dados
Sessão	Comunicação entre hosts
Transporte	Conexão ponto a ponto
Rede	Endereçamento
Enlace	Acesso aos meios
Física	Transmissão binária

Segurança de Redes

- Transmission Control Protocol/Internet Protocol (TCP/IP)

Aplicação	Processos de rede para aplicação
Transporte	Conexão ponto a ponto
Internet	Endereçamento
Enlace	Transmissão binária

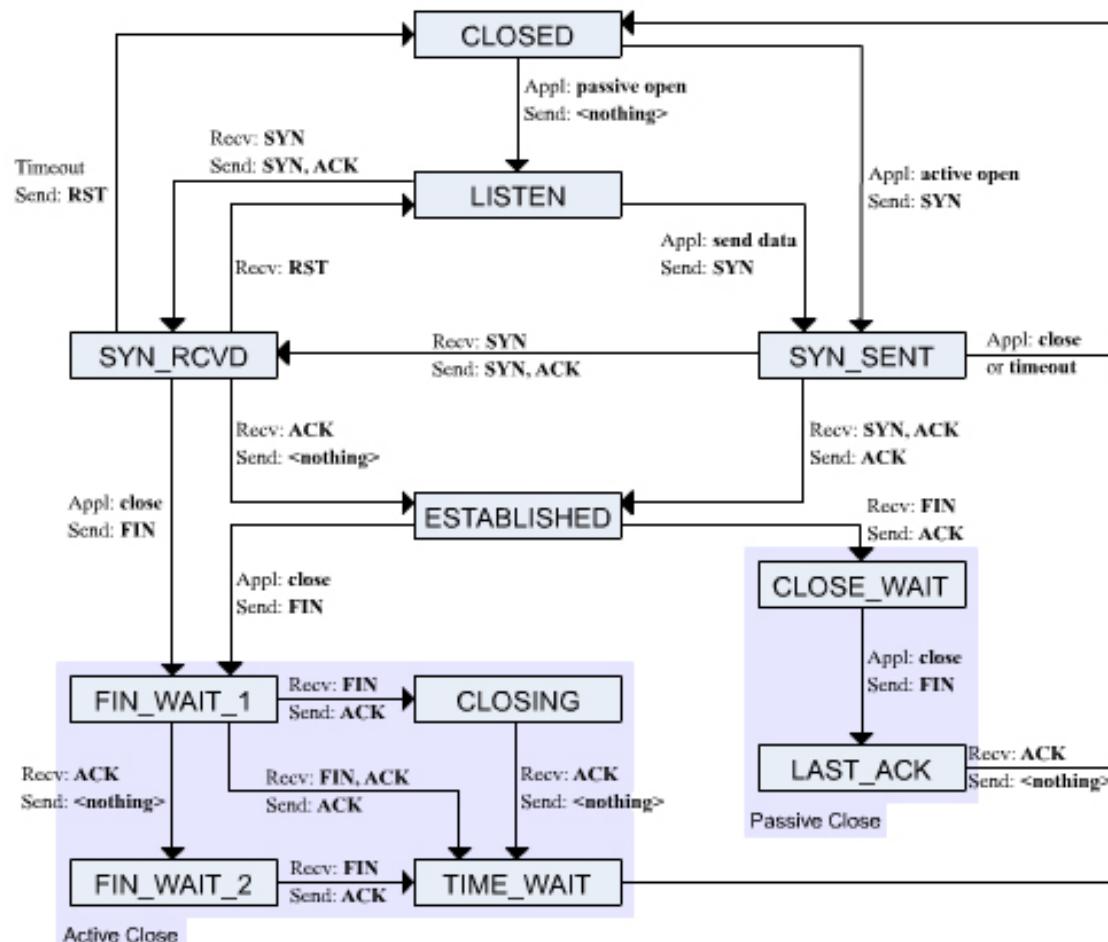
Segurança de Redes

- Transmission Control Protocol/Internet Protocol (TCP/IP)

Aplicação	Mensagens
Transporte	Pacotes
Internet	Datagramas
Enlace	Frames

Segurança de Redes

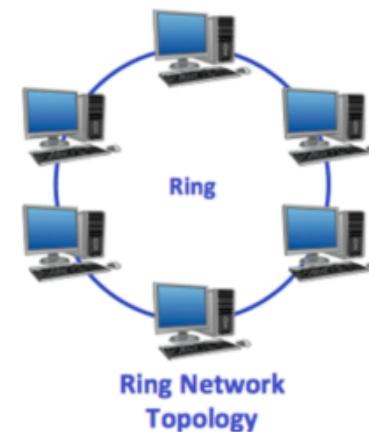
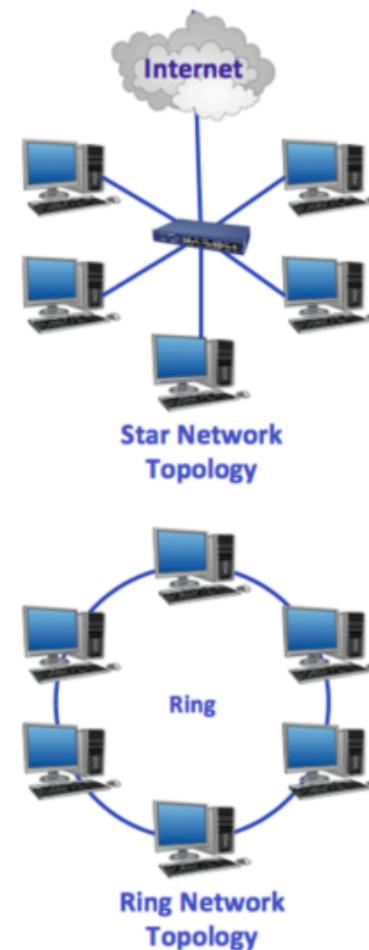
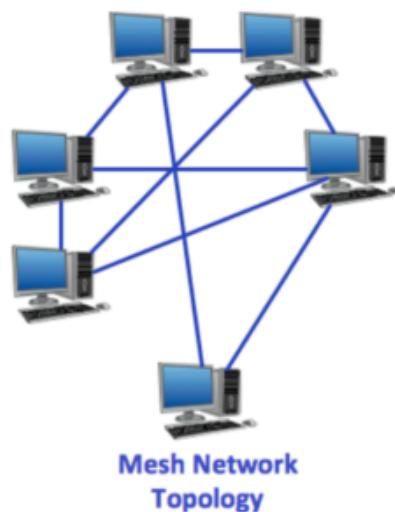
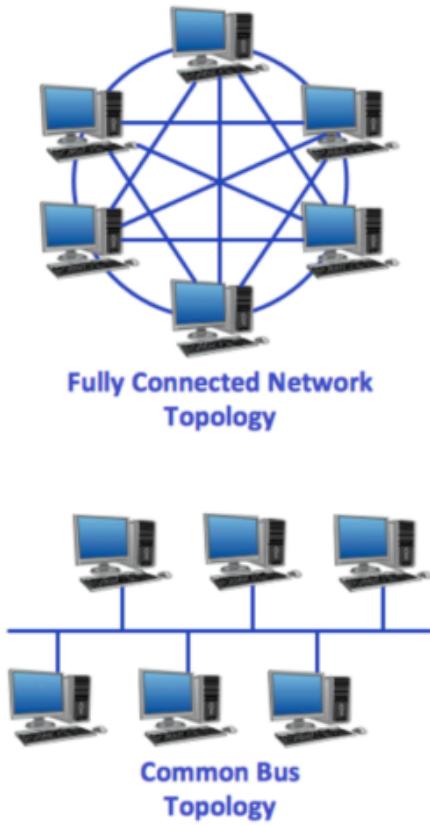
- Máquina de estados finita do TCP/IP



- Protocolos de rede
 - Aplicação
 - BGP, DHCP, DNS, FTP, HTTP, IMAP, LDAP, MGCP, NNTP, NTP, POP, RPC, RIP, SIP, SMTP, SNMP, SSH, Telnet, TLS/SSL, XMPP, ...
 - Transporte
 - TCP, UDP, RTP, DCCP, SCTP, RSVP, ...
 - Internet
 - OSPF, IP (IPv4 e IPv6), ICMP, ICMPv6, ECN, IGMP, IPsec, ...
 - Enlace
 - NDP, ARP, L2TP, PPP, MAC, Ethernet, DSL, RDIS, FDDI, ...

Segurança de Redes

- Topologias de rede



Segurança de Redes

- Preparação do Ambiente
 - Wireshark
 - <https://www.wireshark.org>

Segurança de Redes

- Captura de pacotes de rede
 - <http://www.folha.com.br>
 - <http://testphp.vulnweb.com>

Segurança de Redes

- Simple Mail Transfer Protocol (SMTP)
 - RFC 821
 - Porta 25
 - Comandos
 - helo
 - mail from:<>
 - rcpt to:<>
 - data
 - .

Segurança de Redes

- Preparação do Ambiente
 - Instalar o sendmail
 - sudo apt-get update
 - sudo apt-get install sendmail
 - sudo sendmailconfig

- Post Office Protocol (POP)
 - RFC 1939
 - Porta 110
 - Comandos
 - user
 - pass
 - list
 - retr

- Preparação do Ambiente
 - Instalar o dovecot
 - sudo apt-get update
 - sudo apt-get install dovecot-pop3d
 - sudo vi /etc/dovecot/conf.d/10-auth.conf
 - disable_plaintext_auth = no

Segurança de Redes

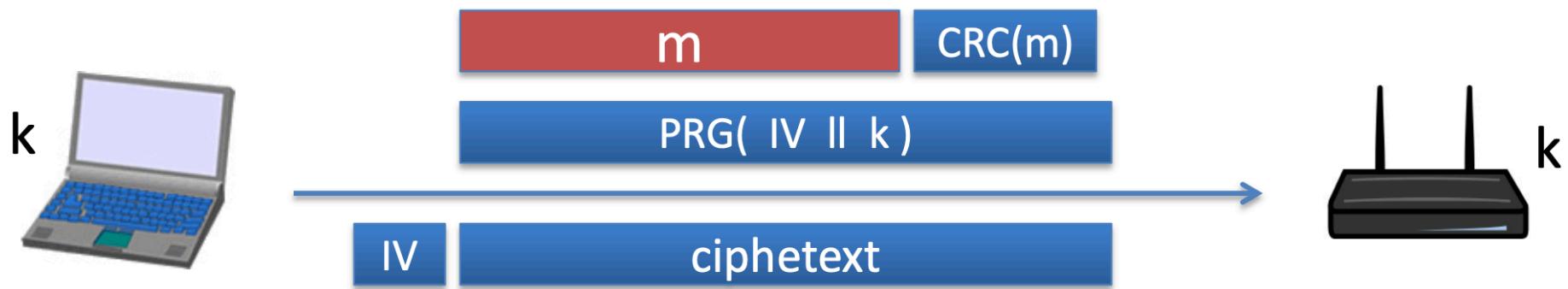
- Captura de pacotes de rede
 - Envio e recebimento de e-mails

Segurança de Redes Sem Fio

Segurança de Redes Sem Fio

EDUCAÇÃO SUPERIOR

- 802.11b WEP



- 802.11b WEP
 - Tamanho da senha: 104 bits
 - Tamanho do IV: 24 bits
 - Começa a repetir o IV depois de 2^{24} frames
 - 16.777.216 frames
 - Chave para o frame 1: $(1 \parallel k)$
 - Chave para o frame 2: $(2 \parallel k)$
 - Chave para o frame 3: $(3 \parallel k)$
 - ...

- 802.11b WEP
 - PRG utilizado: RC4
 - A primeira quebra ocorreu com 1.000.000 de frames
 - Atualmente se quebra com 40.000 frames

Segurança de Redes Sem Fio

EDUCAÇÃO SUPERIOR

- 802.11b WEP
 - Ataques ativos
 - CRC é linear
 - $\forall m, p: \text{CRC}(m \wedge p) == \text{CRC}(m) \wedge \text{CRC}(p)$

WEP ciphertext:



$$XX = 25 \oplus 80$$



- Na decriptação, CRC é válido, porém o criptograma foi adulterado

- Construção melhor



Segurança de Redes Sem Fio

EDUCAÇÃO SUPERIOR

- Construção muito melhor
 - Parar de inventar e usar WPA2

- Invasão de redes sem fio
 - Colocar a placa de rede em modo promíscuo
 - sudo airmon-ng start wlan0
 - Procurar as redes sem fio disponíveis
 - sudo airodump-ng wlan0mon
 - Capturar os pacotes
 - sudo airodump-ng --bssid <id da rede> --chanel 11 -- write [nome do arquivo] wlan0mon
 - Fazer análise estatística dos pacotes capturados
 - sudo aircrack-ng [nome do arquivo]

Firewalls

Firewalls

- Ao se conectar à Internet, três coisas são postas em risco
 - Seus dados
 - A informação que há nos computadores
 - Seus recursos
 - Os computadores propriamente ditos
 - Sua reputação

Firewalls

- Características dos dados que precisam ser protegidas
 - Sigilo
 - Integridade
 - Disponibilidade

Firewalls

- Formas de proteção
 - No security at all
 - Security through obscurity
 - Host security
 - Network security

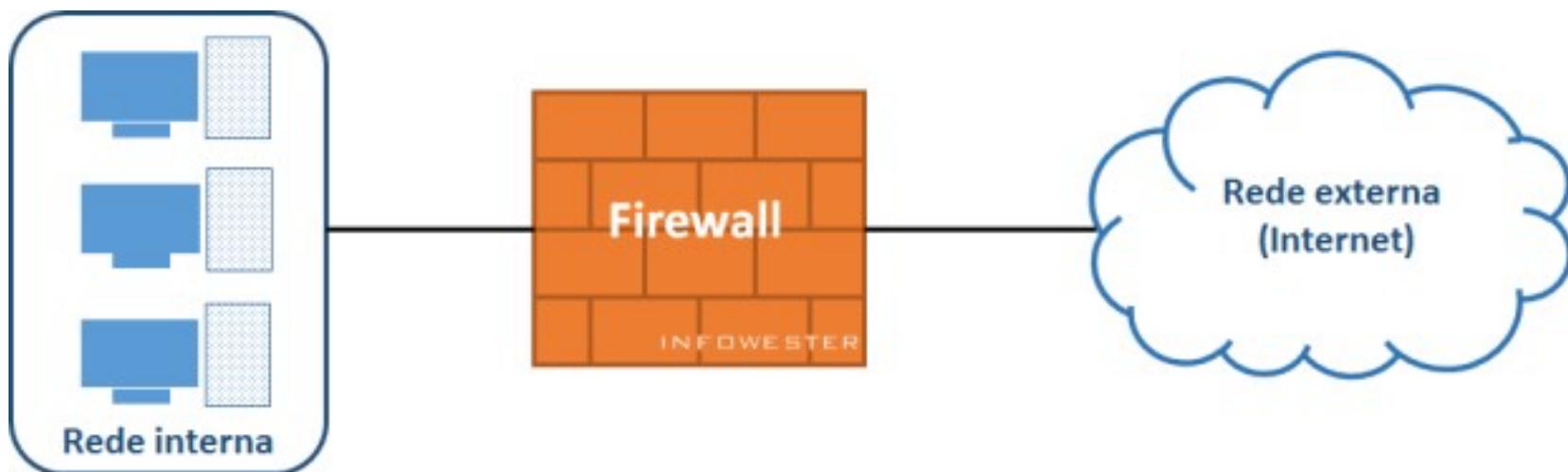
Firewalls

- Firewall
 - Previne que os perigos da Internet invadam e se espalhem na rede interna
 - Restringe as pessoas a entarem em algum ponto cuidadosamente controlado
 - Previne atacantes de chegarem perto das outras defesas que porventura haja
 - Restringe as pessoas de saírem de algum ponto cuidadosamente controlado
 - Normalmente instalado no local onde a rede interna protegida se conecta à Internet

Firewalls

- Firewall
 - Componente ou conjunto de componentes que restringem o acesso entre uma rede protegida e a Internet; ou entre outros conjuntos de rede

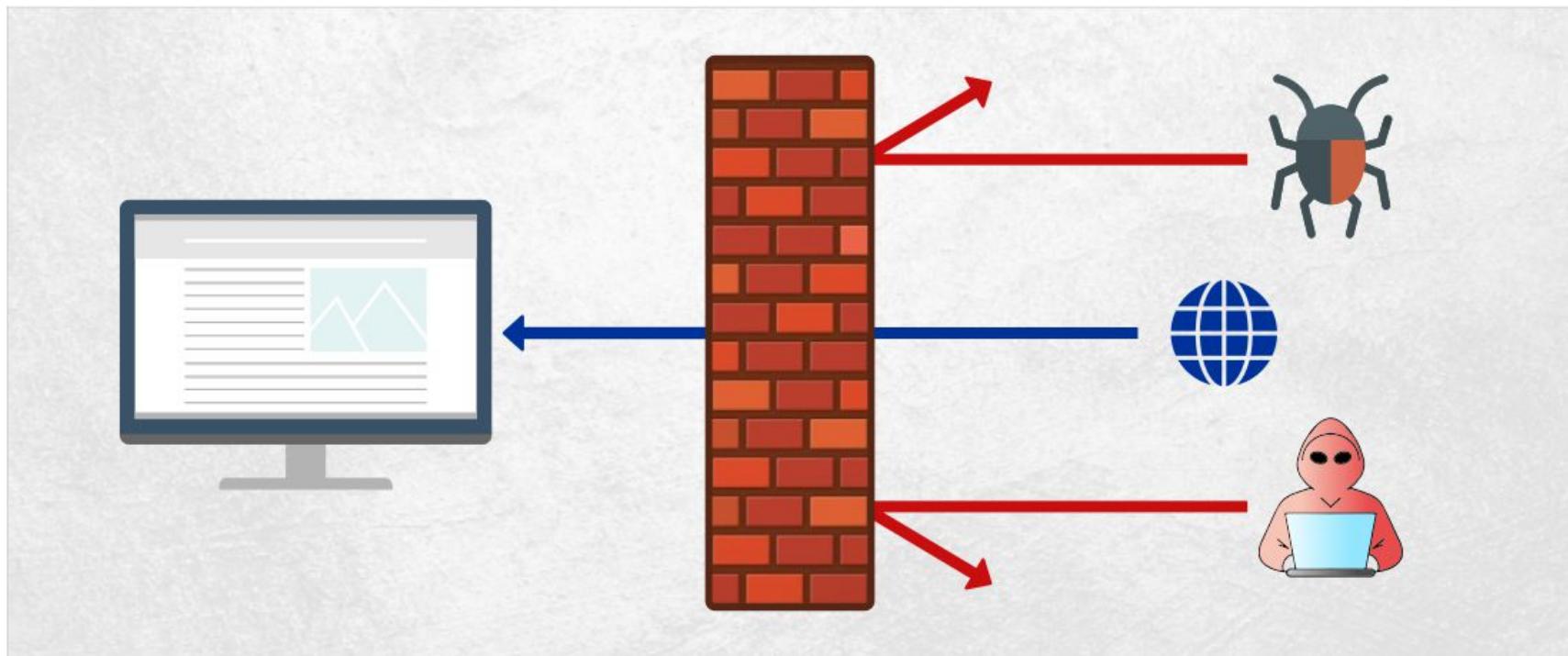
Firewalls



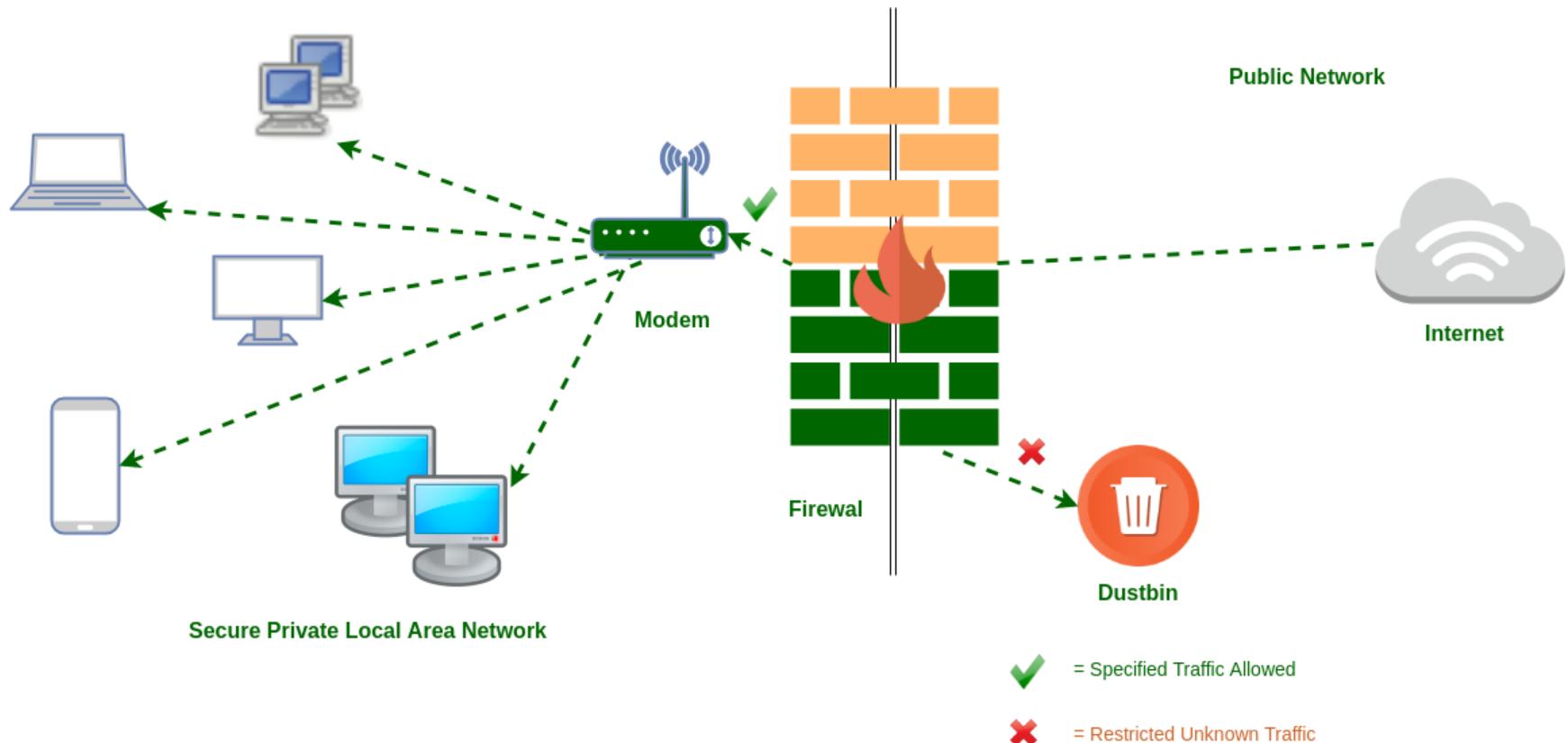
Firewalls



Firewalls



Firewalls



Firewalls



Firewalls

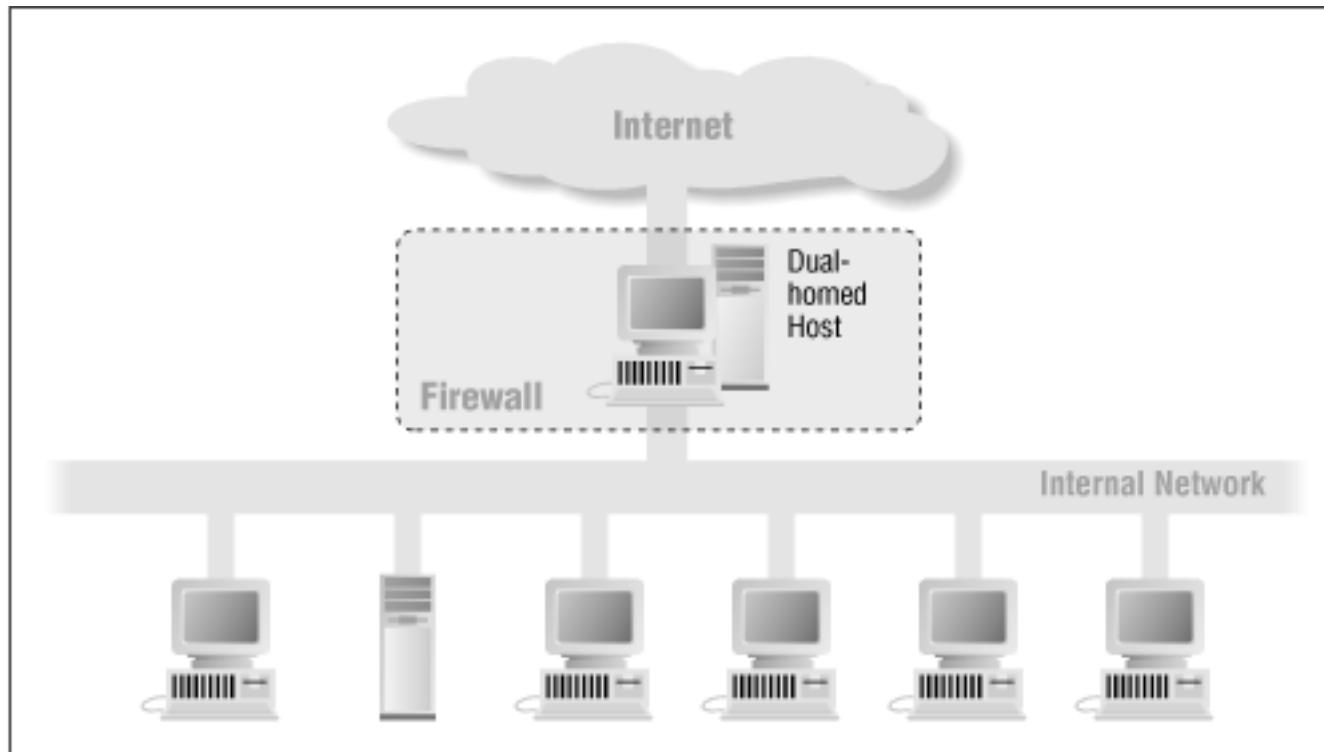
- O que um firewall pode fazer
 - Ser o foco das decisões de segurança
 - Fortalecer a política de segurança
 - Logar a atividade da Internet com efetividade
 - Limitar a exposição da rede

Firewalls

- O que um firewall NÃO pode fazer
 - Proteger contra atividade maliciosa interna
 - Proteger contra conexões que não passem por ele
 - Proteger contra ameaças completamente novas
 - Proteger contra virus

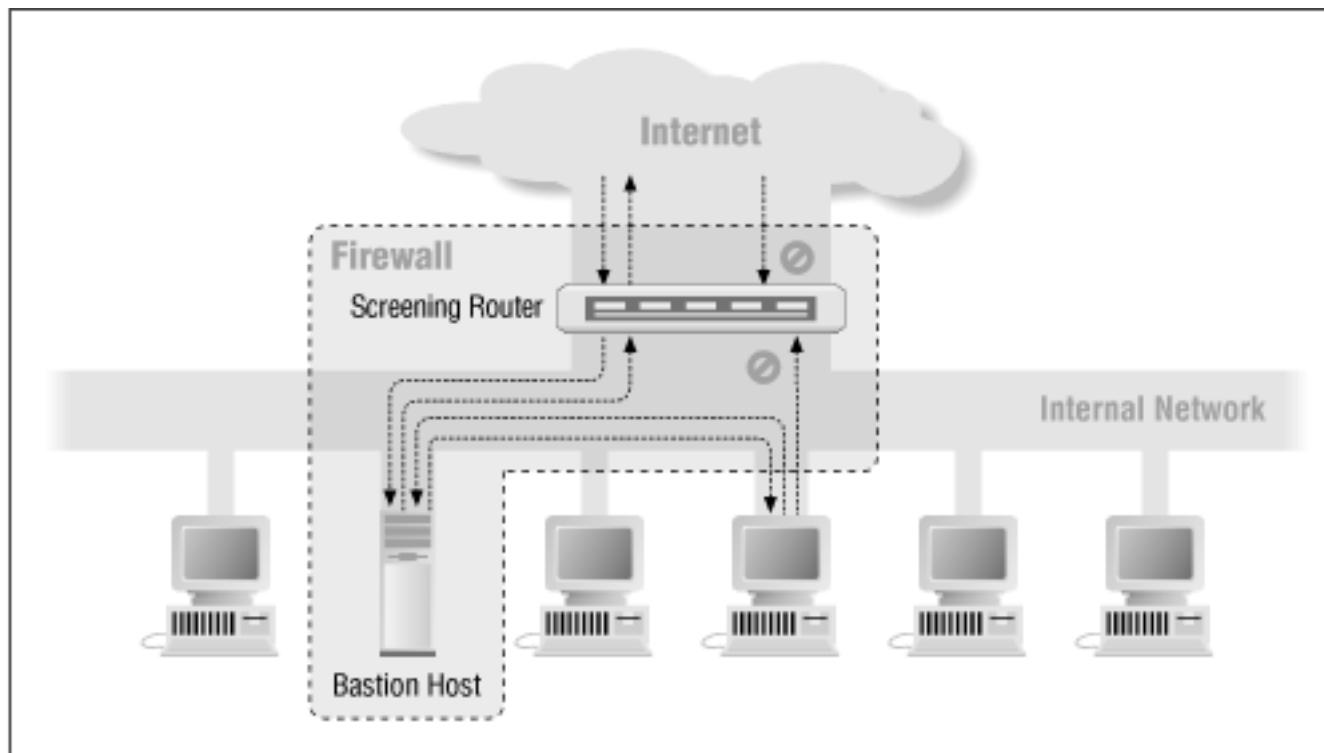
Firewalls

- Arquitetura Dual-Homed Host



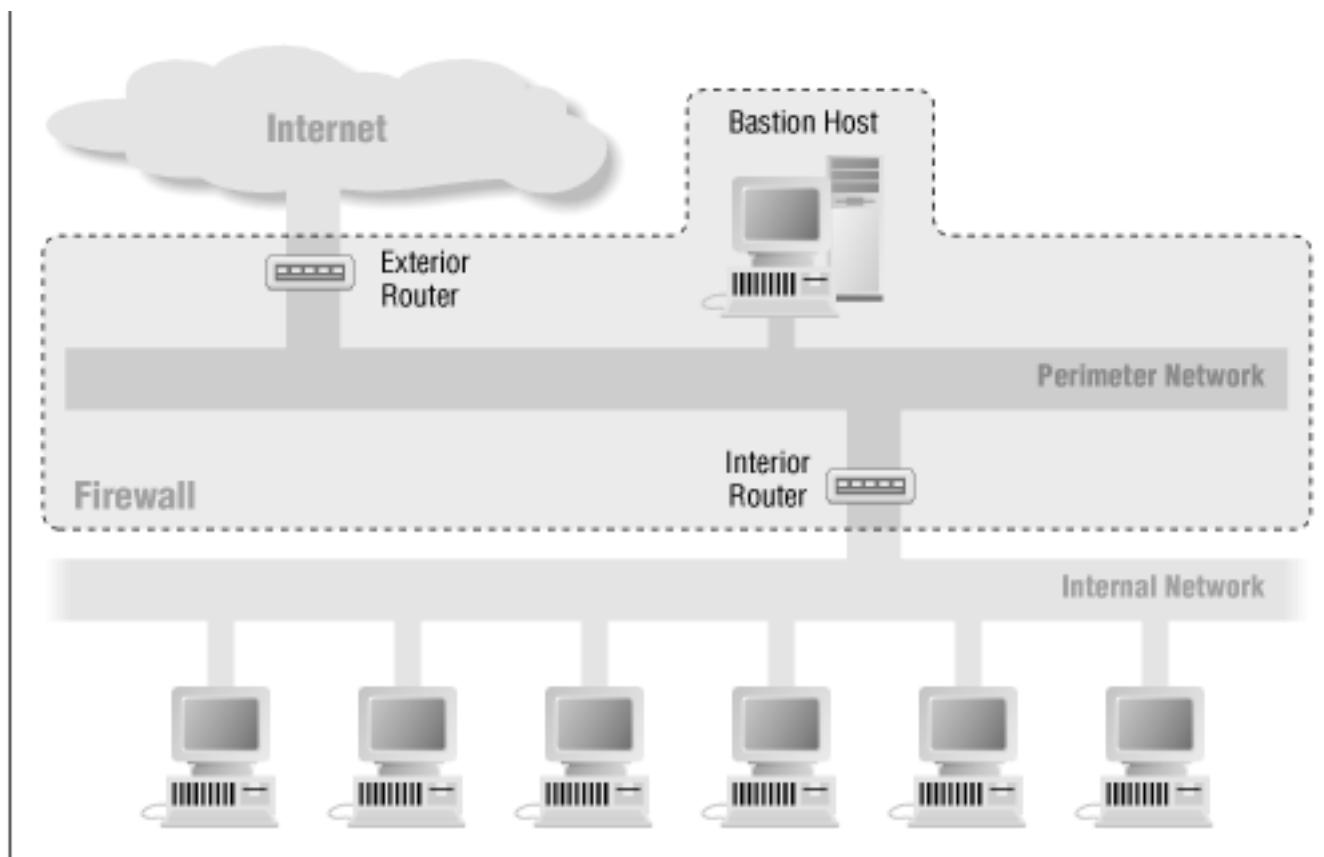
Firewalls

- Arquitetura Screened Host



Firewalls

- Arquitetura Screened Subnet



Firewalls

- Variações arquiteturais
 - Múltiplos bastion hosts
 - Único roteador (interno e externo)
 - Múltiplos roteadores externos
 - Múltiplos firewalls

Firewalls

- Filtragem de pacotes
 - Controle do tráfego com base
 - No endereço do remetente
 - No endereço do destinatário
 - Nos protocolos de aplicação utilizados
 - A maior parte dos sistemas de filtragem de pacotes não tomam decisões com base no conteúdo dos pacotes, porém nos metadados
 - Firewall da CheckPoint é exceção

Firewalls

- Filtragem de pacotes
 - Exemplos possíveis
 - Não permita que alguém use Netcat para login de fora da rede
 - Permita que qualquer um envie e-mail por SMTP
 - Permita que uma estação externa específica envie notícias via NNTP, mas proíba que qualquer outra estação o faça
 - Exemplos não possíveis
 - Esse usuário específico pode usar Netcat para login de fora da rede, enquanto outros usuários não podem
 - Permita a transmissão via FTP desse arquivo, não daqueles outros arquivos

Firewalls

- Firewall é um conjunto de regras com endereços de origem, destino, porta
 - Deny: descarta o pacote de rede
 - Allow: permite a passagem do pacote de rede

Firewalls

- Diferença entre proxy e firewall
 - Firewall permite ou impede pacotes de rede com base nas definições de segurança
 - Camada de rede
 - Proxy intermedia as conexões para diversos fins tais como, anonimato, cache, filtro de navegação
 - Camada de aplicação
 - Ambos contribuem para a segurança da informação corporativa

Firewalls

- Firewall Aker
 - Universidade de Brasília (1997)

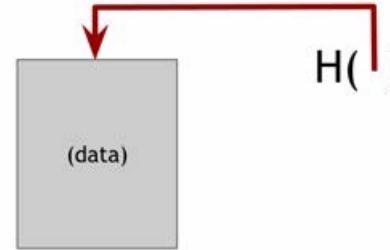
Criptomoedas

Criptomoedas

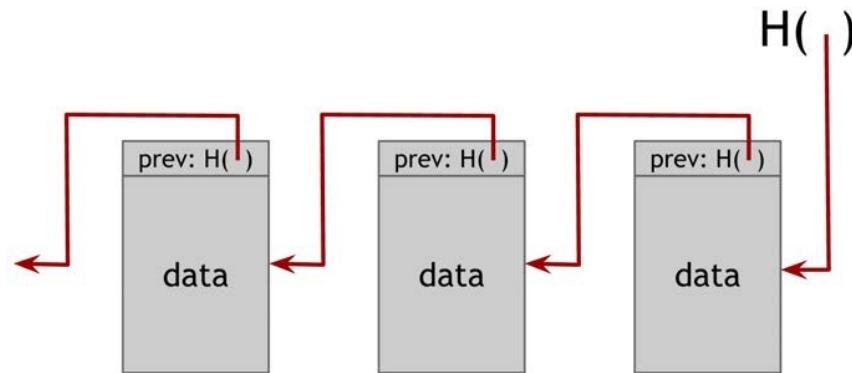
- O que é valor ?
- O que representa o valor ?
- O que é lastro ?
- Qual a segurança do papel moeda ?
- Ataque de double-spending

Criptomoedas

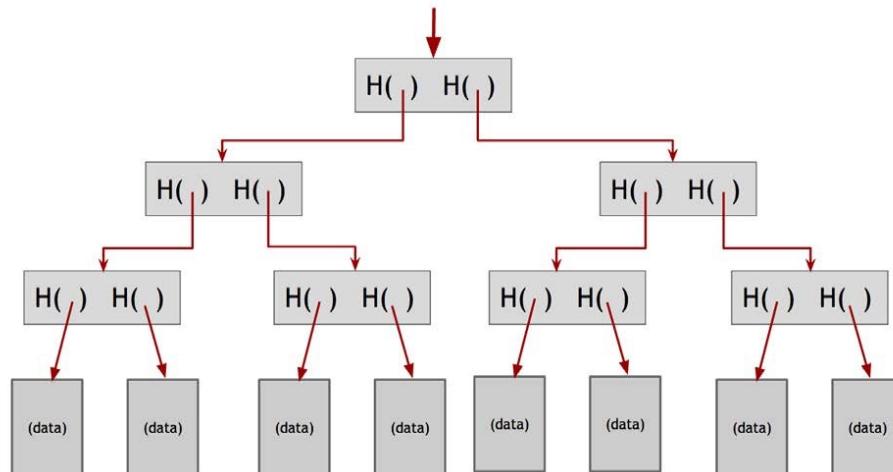
- Ponteiro de resumo



- Cadeia de blocos



- Árvore de Merkel

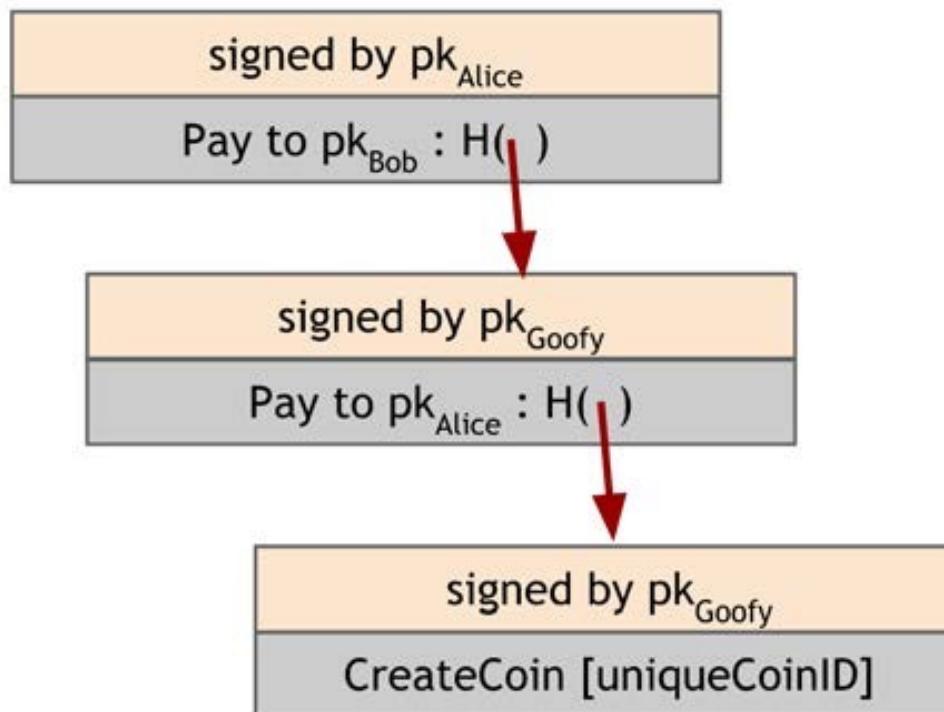


Criptomoedas

- GoofyCoin
 - O Pateta pode criar novas moedas quando quiser e bem entender, e essas moedas pertencem a ele
 - Gera um identificador único de moeda
 - Constrói uma sentença “CreateCoin[UniqueCoinID]”
 - Assina a sentença com sua chave secreta
 - Quem quer que possua uma moeda, pode transferi-la a quem quiser
 - Cria uma sentença “PayCoin to X”

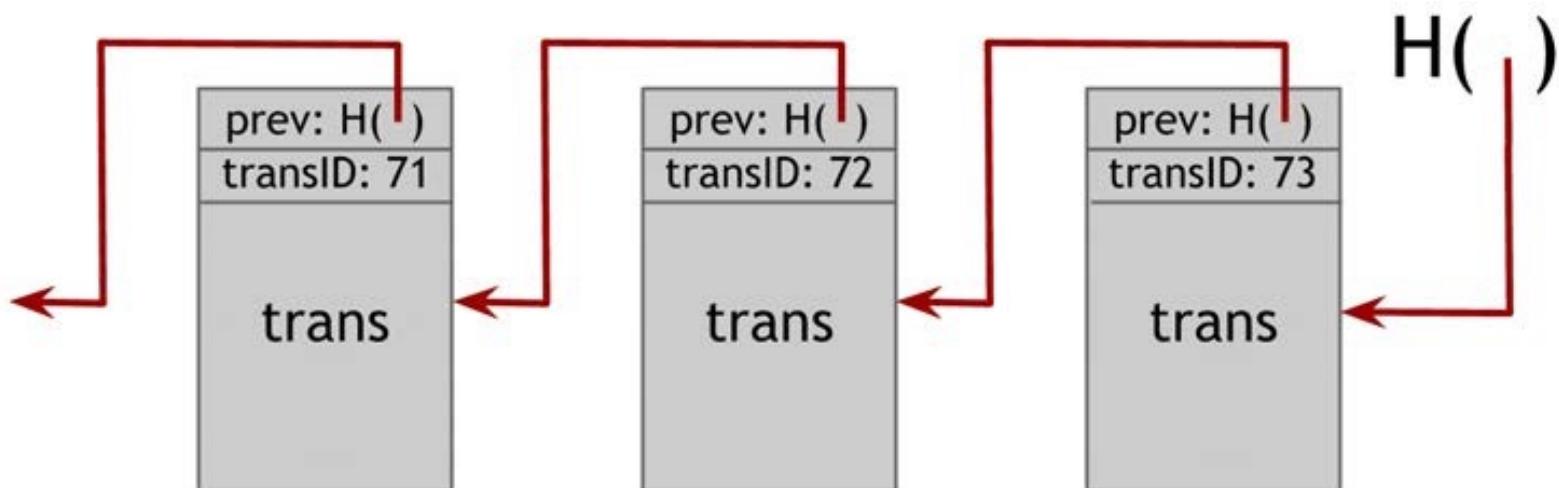
Criptomoedas

- GoofyCoin



Criptomoedas

- ScroogeCoin
 - O Tio Patinhas publica um histórico de todas as transações que já houve.



Criptomoedas

- ScroogeCoin
 - CreateCoin
 - Múltiplas moedas na mesma transação
 - PayCoin
 - As moedas consumidas são válidas, ou seja, foram criadas em transações anteriores
 - As moedas consumidas não foram consumidas anteriormente em transações anteriores
 - O valor total das moedas que entram na transação é precisamente igual ao valor total que sai
 - A transação é assinada por todos os proprietários das moedas consumidas

Criptomoedas

- ScroogeCoin
 - Moedas são imutáveis: elas nunca são mudadas, subdivididas ou combinadas
 - Cada moeda é criada em uma transação, e posteriormente consumida em outra transação
 - Conquanto o problema do double-spending esteja resolvido, outro problema emerge: o poder centralizado do Tio Patinhas

Criptomoedas

- Programa implementação da árvore de Merkel

Bitcoin



Bitcoin

- Satoshi Nakamoto
 - Bitcoin: A Peer-to-Peer Electronic Cash System
 - Novembro de 2008

Bitcoin

- Descentralização
 - Quem mantém o histórico de transações ?
 - Quem tem autoridade sobre quais transações são válidas ?
 - Quem cria novos Bitcoins ?
 - Quem determina como as regras do sistema mudam ?
 - Como os Bitcoins adquirem valor de troca ?

- Consenso distribuído
 - Há vários nós cada qual com um valor de entrada. Alguns desses nós estão errados ou são maliciosos. Um protocolo de consenso distribuído tem duas propriedades:
 - Deve terminar com todos os nós honestos concordando com o valor
 - O valor deve ter sido gerado por um nó honesto

- Consenso distribuído no Bitcoin
 - Todos os nós da rede devem manter uma cópia atualizada da Block Chain
 - Novas transações devem ser divulgadas e espalhadas para todos os nós da rede
 - Cada nó seleciona as transações que quiser e constrói um bloco com elas
 - Em cada rodada, um nó selecionado randomicamente divulga o seu bloco
 - Outros nós aceitam o bloco somente se todas as transações nele contidas forem válidas (análise de double-spending, assinaturas válidas, ...)
 - Os nós da rede expressam sua aceitação do bloco incluindo seu hash no próximo bloco que eles criarem

- A proteção contra transações inválidas é inteiramente criptográfica
- O consenso apresenta um reforço, considerando que um bloco inválido não vai ser acrescentado à Block Chain
- Por outro lado, a proteção contra double-spending é puramente consensual, porque ambas transações são válidas da perspectiva estritamente criptográfica
 - Bloco órfão

Bitcoin

- Exemplificação gráfica
 - <https://andersbrownworth.com/blockchain/blockchain>

Bitcoin

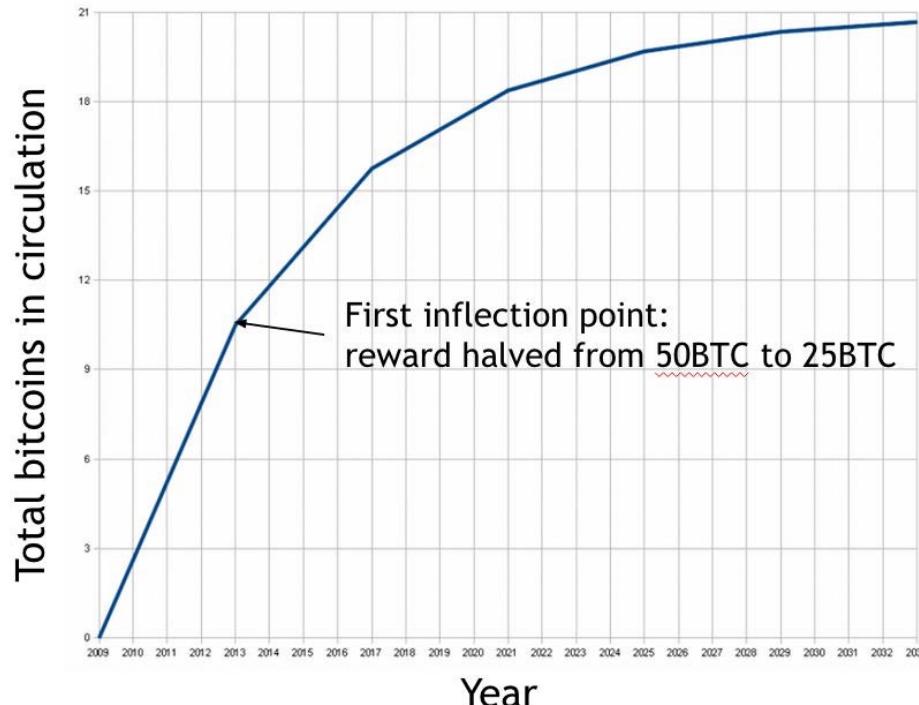
- Programa implementação da Block Chain

Bitcoin



Bitcoin

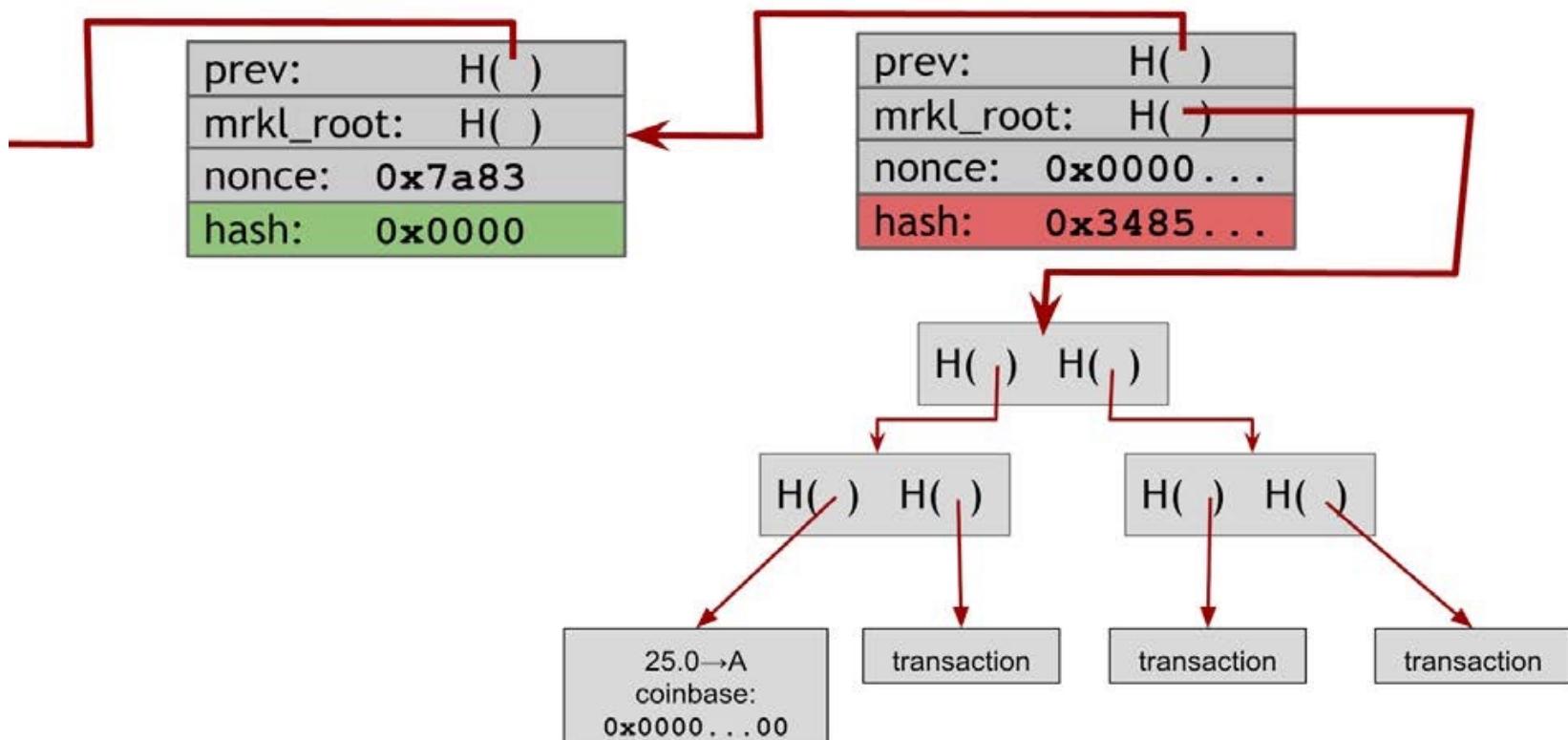
- Remuneração do bloco
 - Mineração



- Taxa de transação

- Mineração
 - O hash do bloco deve ser menor que um limite estabelecido
 - Em março de 2015 o limite era exatamente:
0000000000000000172EC00000000000000000000000000
00000000000000000000000000
 - Ou seja, o hash de 256 bits escrito em hexadecimal deve começar com 16 zeros (64 bits zerados em sequencia)
 - Em 2021 o limite eram 19 zeros
 - Ou seja, o hash de 256 bits escrito em hexadecimal deve começar com 19 zeros (76 bits zerados em sequencia)

- Mineração



Bitcoin

- Mineração



Bitcoin

- Mineração



Bitcoin

CEUB

EDUCAÇÃO SUPERIOR

- Mineração



Bitcoin

- Programa mineração de Bitcoins

Bitcoin



Bitcoin

- Registro de transações
 - Transação 1 → assinada pelo minerador
Inputs 0
Outputs 25 → Alice
 - Transação 2 → assinada por Alice
Inputs Transação 1
Outputs 17 → Bob
8 → Alice

- Registro de transações
 - Transação 3 → assinada por Bob
Inputs Transação 2
Outputs 8 → Carol
 9 → Bob
 - Transação 4 → assinada por Alice
Inputs Transação 2
Outputs 6 → David
 2 → Alice

- Mudança de endereço
 - Anonimidade
- Verificação eficiente
 - Não precisa varrer a Block Chain toda
- Consolidação de fundos
 - Duas transações de entrada para a mesma conta de saída
- Pagamentos conjuntos
 - Exige assinatura de todos os participantes pagantes

- Exemplo real de transação na Block Chain

```
{  
    "hash":"5a42590fbe0a90ee8e8747244d6c84f0db1a3a24e8f1b95b10c9e050990b8b6b",  
    "ver":1,  
    "vin_sz":2,  
    "vout_sz":1,  
    "lock_time":0,  
    "size":404,  
    "in":[  
        {  
            "prev_out":{  
                "hash":"3be4ac9728a0823cf5e2deb2e86fc0bd2aa503a91d307b42ba76117d79280260",  
                "n":0  
            },  
            "scriptSig":"30440....3f3a4ce81"  
        },  
        {  
            "prev_out":{  
                "hash":"7508e6ab259b4df0fd5147bab0c949d81473db4518f81afc5c3f52f91ff6b34e",  
                "n":0  
            },  
            "scriptSig":"304602210....3f3a4ce81"  
        }  
    ],  
    "out": [  
        {  
            "value": "10.12287097",  
            "scriptPubKey": "OP_DUP OP_HASH160 69e02e18b5705a05dd6b28ed517716c894b3d42e OP_EQUALVERIFY OP_CHECKSIG"  
        }  
    ]  
}
```

- Bitcoin scripting language
 - Similar à linguagem de programação Forth
 - Linguagem antiga, simples, baseada em pilha
 - Não possui laços
 - Proteção para a Block Chain
 - Primitivas criptográficas nativamente implementadas

OP_DUP	Duplicates the top item on the stack
OP_HASH160	Hashes twice: first using SHA-256 and then RIPEMD-160
OP_EQUALVERIFY	Returns true if the inputs are equal. Returns false and marks the transaction as invalid if they are unequal
OP_CHECKSIG	Checks that the input signature is a valid signature using the input public key for the hash of the current transaction
OP_CHECKMULTISIG	Checks that the k signatures on the transaction are valid signatures from k of the specified public keys.

- Transações com garantia de depósito
 - Suponha que Alice esteja comprando algo físico da loja online de Bob e queira pagar com Bitcoins
 - Alice só quer transferir os Bitcoins quando o produto chegar
 - Bob só quer enviar o produto quando os Bitcoins forem transferidos
 - Terceira parte para arbitrar a transação
 - Alice cria uma transação MULTISIG (multi-assinatura) onde há 3 (três) pessoas marcadas para potencialmente assinar, porém apenas 2 (duas) são necessárias para liberar os fundos

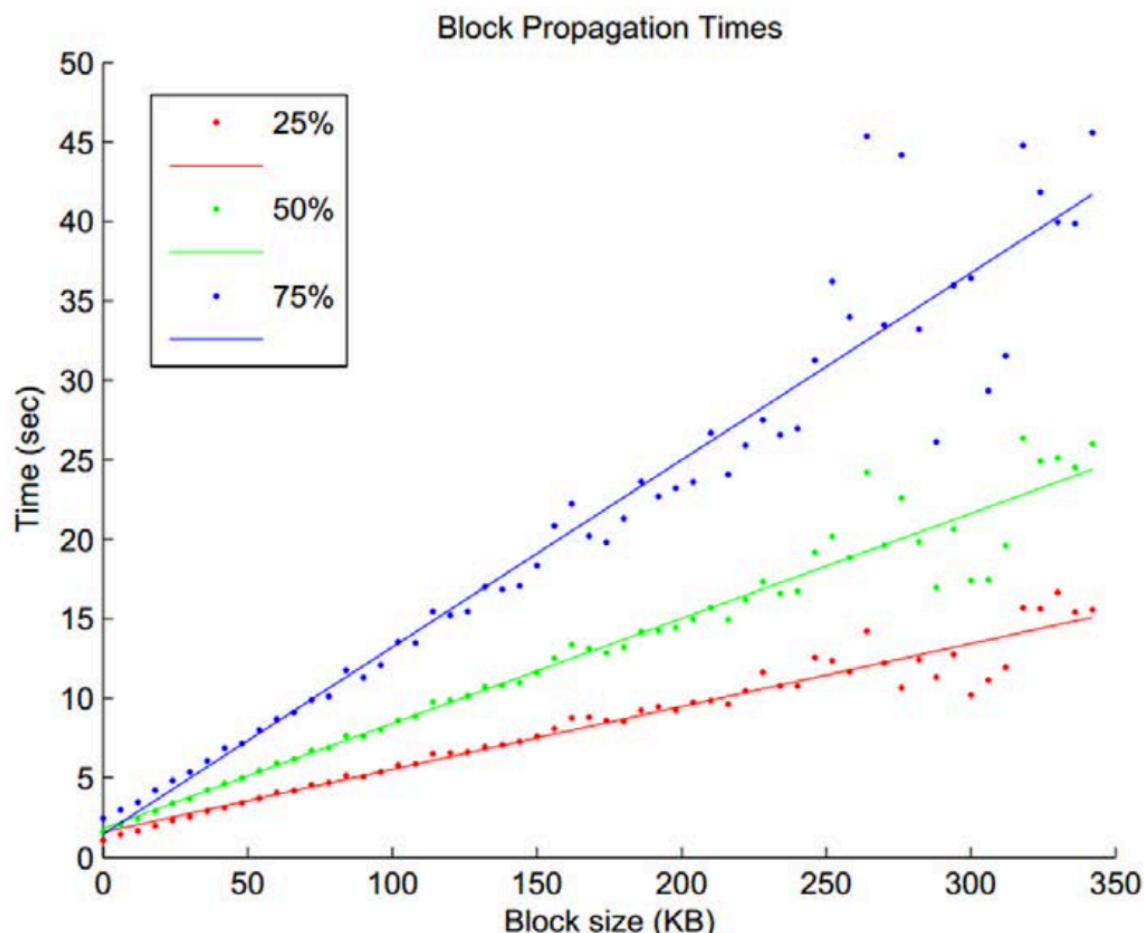
- Endereços verdes
 - Considerando que, em média, um bloco novo surge a cada 10 (dez) minutos
 - Considerando que, em média, deve-se aguardar a confirmação de 6 (seis) blocos para garantir uma transação
 - Conclui-se, portanto, que uma operação com Bitcoins demora 1 (uma) hora, em média, para ser confirmada
 - Dá pra beber cerveja no boteco pagando com Bitcoin ?!?!?!

- Endereços verdes
 - Utilizar um intermediário financeiro (banco, corretora, ...)
 - O intermediário financeiro tem reputação, confiança pública, e não apresenta, em todo o histórico da Block Chain, nenhuma tentativa de double-spending
 - O comprador transfere para o intermediário
 - O intermediário transfere para o vendedor a partir de um de seus endereços verdes
 - O vendedor aplica a confiança estabelecida no intermediário, e conclui a venda no mundo real imediatamente

- Endereços verdes
 - Garantia não vem da segurança do Bitcoin, porém da segurança do mundo real
 - Intermediários financeiros mais importantes
 - Instawallet
 - Mt. Gox
 - Ambos colapsaram

Bitcoin

- A rede do Bitcoin



Bitcoin

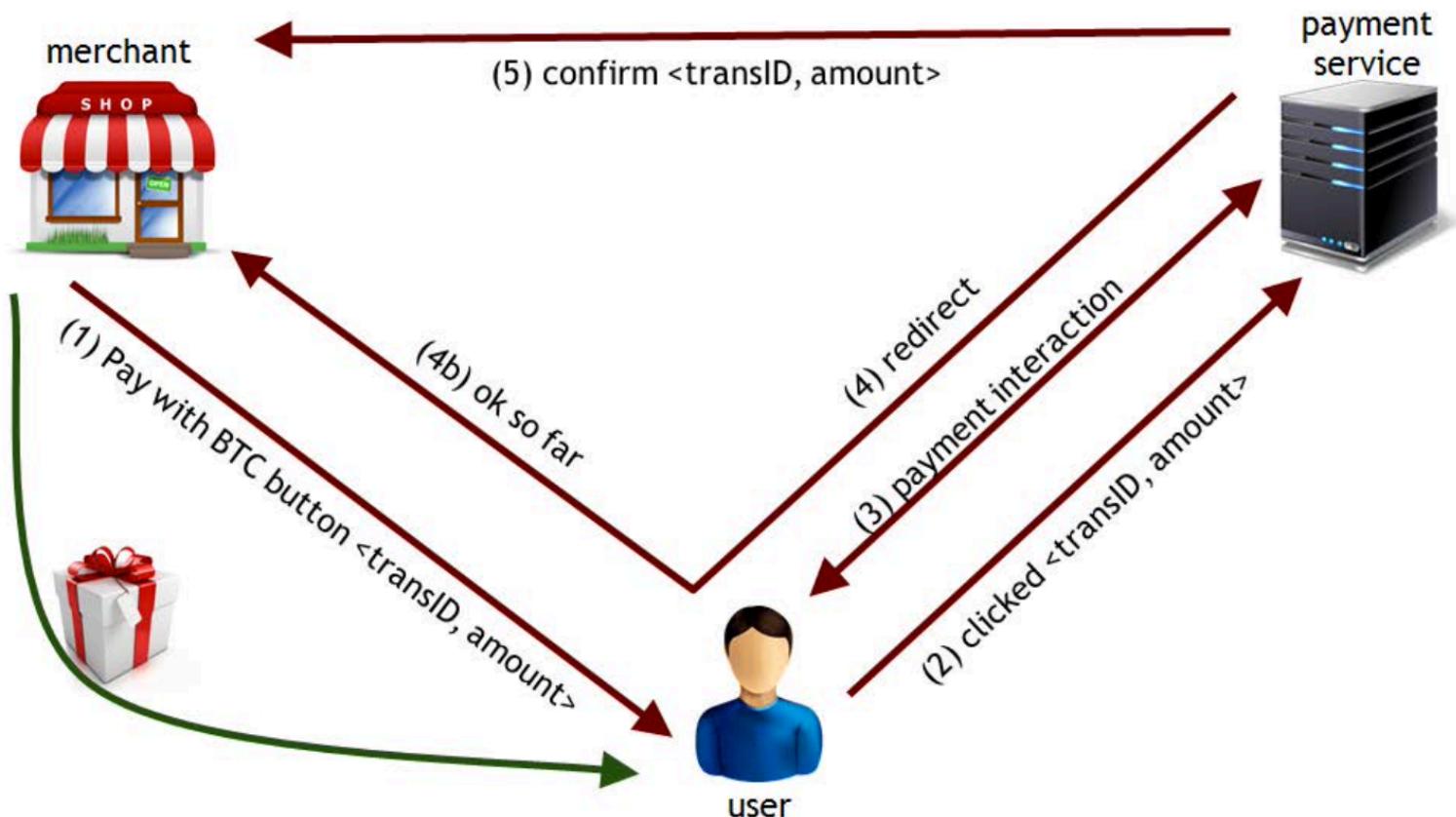
- A limitação da quantidade de Bitcoins disponíveis tem graves implicações econômico-financeiras

- Armazenamento de Bitcoins
 - Armazenar Bitcoins resume-se a armazenar e gerenciar chaves secretas de criptografia assimétrica
 - Diferentes abordagens para o gerenciamento de chaves oferecem diferentes compensações entre disponibilidade, segurança e conveniência

- Armazenamento de Bitcoins
 - Bitcoin Wallets
 - Base58
 - QR code
 - Regular expressions
 - ($[^\wedge 0-9a-zA-Z][13][a-km-zA-HJ-NP-Z1-9]\{25,34\}[^0-9a-zA-Z]$)
 - ($[^\wedge 0-9a-zA-Z]bc1[a-zA-Z0-9]\{20,87\}[^0-9a-zA-Z]$)
 - Seed phrases

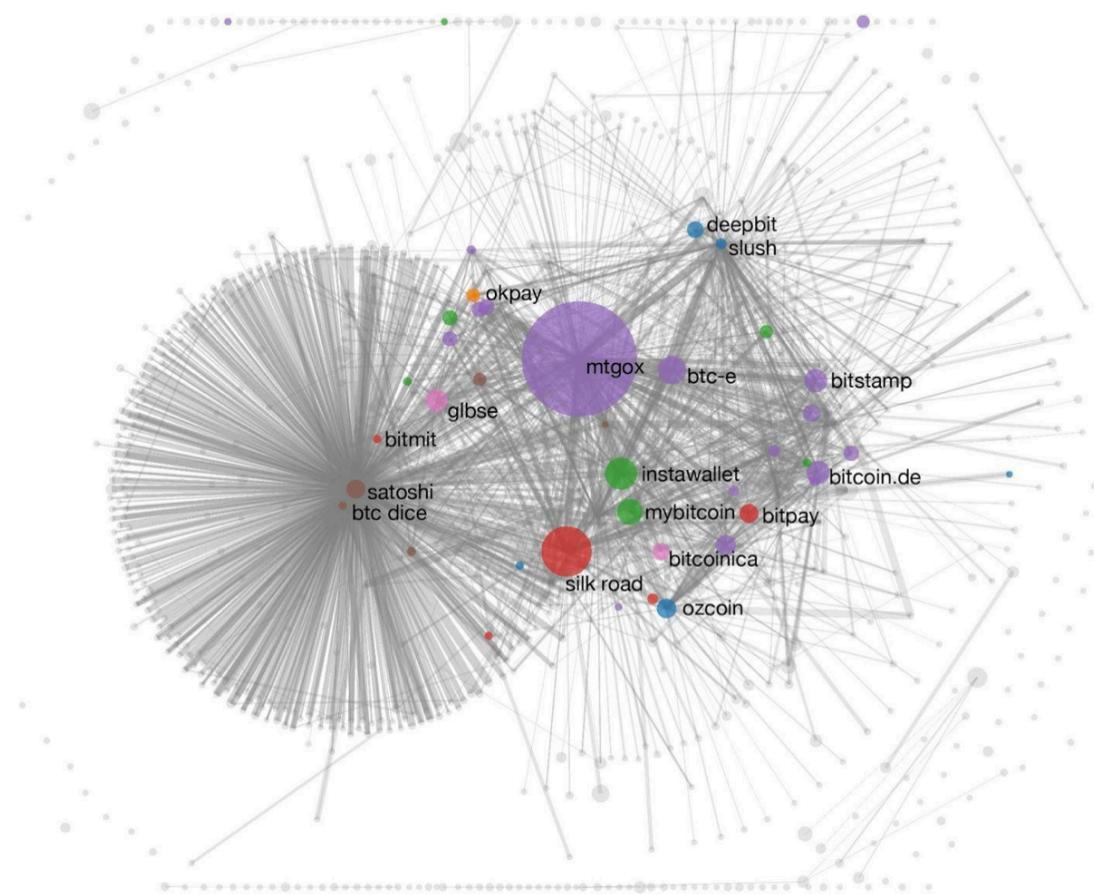
Bitcoin

- Processo de pagamento



Bitcoin

- Anonimidade



Bitcoin

CEUB

EDUCAÇÃO SUPERIOR

- Comunidade
- Política
- Regulamentação
- Ecologia

Bitcoin

- Economia globalizada, moeda descentralizada
- O Bitcoin é comprovadamente seguro
- Crimes cibernéticos
- Área de pesquisa da Interpol

Bitcoin

- Bitcoin core
 - <https://github.com/bitcoin/bitcoin>
 - <https://bitcoincore.org/en/download/>
 - 400 GB (quatrocentos gigabytes) Block Chain
 - De 5 GB a 10 GB (cinco a dez gigabytes) por mês

Altcoins

Altcoins

- Ethereum (ETH)
 - Vitalik Buterin
 - Janeiro de 2014
 - Ethereum Virtual Machine (EVM)
 - Smart contracts
 - Protocolo autoexecutável que proporciona confiabilidade em transações online

Altcoins

- Ethereum (ETH)
 - Nuvem de execução de escala planetária na qual usuários pagam pelo recurso utilizado
 - Transação
 - Registro
 - Execução de código distribuído
 - Assinatura de contrato digital
 - Qualquer coisa que possa ser programada
 - Ether

Altcoins

- Ethereum (ETH)
 - Hard fork na Block Chain em 2016 porque um vagabundo roubou US\$ 50.000.000,00 (cinquenta milhões de dólares) em Ethers
 - Criptografia mal programada dá nisso...
 - <https://github.com/ethereum>
 - <https://ethereum.org/en/>

Altcoins

- Litecoin (LTC)
 - Charlie Lee
 - Colaborador do Google
 - Outubro de 2011
 - Exatamente igual ao Bitcoin menos 3 (três) detalhes
 - Cada bloco é processado em 2,5min (dois minutos e meio), em média, ao contrário dos 10min (dez minutos) do Bitcoin
 - A rede irá produzir 84.000.000 (oitenta e quatro milhões) de Litecoins, 4 (quatro) vezes mais do que a quantidade máxima de Bitcoins
 - Prova de trabalho usa uma função sequencial de memória rígida (scrypt), ao invés do SHA-256

Altcoins

- Litecoin (LTC)
 - <https://litecoin.org>

Altcoins

- Ripple (XRP)
 - Jed McCaleb → concepção
 - Criador do eDonkey
 - Arthur Britto, David Schwartz, Ryan Fugger → desenvolvimento
 - 2012
 - Transferência de fundos
 - Câmbio monetário
 - <https://ripple.com>

Altcoins

- Bitcoin Cash (BCH)
 - Agosto de 2017
 - Hard fork na Block Chain do Bitcoin para acomodar blocos de tamanho maior
 - Controvérsia do tamanho do bloco
 - <https://bitcoincash.org>

Altcoins

- Tether Dólar (USDT)
 - J.R. Willett
 - Publicação de um artigo argumentando que é possível criar novas moedas a partir do protocolo do Bitcoin
 - Janeiro de 2012
 - Stablecoin lastreada no Dólar
 - New York Attorney General: "Tether's claims that its virtual currency was fully backed by U.S. dollars at all times was a lie"
 - <https://tether.to>

Altcoins

- Namecoin (NMC)
 - Dezembro de 2010
 - Hard fork na Block Chain do Bitcoin sem nada mudar (?!)
 - Foco na anonimidade de DNS e identidade
 - É possível minerar blocos para ambas Block Chains simultaneamente
 - <https://www.namecoin.org>

- Dogecoin (D)
 - Billy Markus
 - Colaborador da IBM
 - Jackson Palmer
 - Colaborador da Adobe
 - Dezembro de 2013
 - Prova de trabalho usa uma função sequencial de memória rígida (scrypt)
 - Cada bloco é processado em 1min (um minuto)

- Dogecoin (D)
 - Em 2013 um vagabundo roubou milhões de moedas da rede
 - Criptografia mal programada dá nisso...
 - Comunidade lançou a iniciativa “SaveDogemas”
 - Doação de moedas a quem foi roubado
 - Em um mês todo o dinheiro roubado foi arrecadado e distribuído

Altcoins

- Dogecoin (D)
 - 800% (oitocentos porcento) de ganho de valor em 24 (vinte e quatro) horas em Janeiro de 2021
 - Efeito Elon Musk
 - <https://dogecoin.com>

Votação Eletrônica

Votação Eletrônica

- Votação computadorizada não pode ser utilizada em eleições gerais a não ser que haja um protocolo que garanta:
 - Privacidade individual
 - Prevenção de fraude

- Requisitos mínimos
 - Apenas votantes autorizados conseguem votar
 - Ninguém consegue votar mais de uma vez
 - Ninguém consegue determinar o voto de qualquer pessoa
 - Ninguém consegue duplicar o voto de qualquer pessoa
 - Ninguém consegue mudar o voto de qualquer pessoa
 - Todos os votantes têm a garantia de que seu voto foi contabilizado na tabulação final

Votação Eletrônica

- Protocolo de votação simplista
 - Votante
 - Encripta seu voto com a chave pública da instalação central de tabulação (ICT)
 - Envia seu voto a ICT
 - ICT
 - Decripta o voto
 - Contabiliza o voto
 - Publica o resultado da eleição ao final

- Protocolo de votação simplista melhorado
 - Votante
 - Assina seu voto com sua chave secreta
 - Encripta seu voto assinado com a chave pública da ICT
 - Envia seu voto a ICT
 - ICT
 - Decriptua o voto
 - Verifica a assinatura
 - Contabiliza o voto
 - Publica o resultado da eleição ao final

Votação Eletrônica

CEUB

EDUCAÇÃO SUPERIOR

- Programa votação

Votação Eletrônica

Votação Eletrônica

- Protocolo de assinatura cega
 - Bob
 - Prepara n documentos
 - Aplica um fator de ocultação (FO) para ocultar o conteúdo de cada documento
 - Caso o algoritmo de assinatura permita, pode ser a multiplicação por um número randômico
 - $\text{Sign}(m * \text{FO}) == \text{Sign}(m) * \text{FO}$
 - Envia todos os documentos a Alice
 - Alice
 - Escolhe n-1 documentos aleatoriamente e pede a Bob o FO para cada um deles

Votação Eletrônica

- Protocolo de assinatura cega
 - Bob
 - Envia a Alice os respectivos FOs
 - Alice
 - Abre cada um dos $n-1$ documentos e os verifica
 - Assina o último documento, aquele que ela não abriu, ou seja, assinou à cega, e o envia a Bob
 - Bob
 - Remove o FO e tem um documento assinado por Alice que ela não conhece o conteúdo

- Protocolo de votação com assinatura cega
 - Votante
 - Gera 10 (dez) conjuntos de mensagens
 - Cada mensagem possui um identificador randômico
 - Cada mensagem é um voto válido para cada candidato da eleição
 - Executa o protocolo de assinatura cega com a ICT
 - Envia os 10 (dez) conjuntos
 - ICT escolhe 9 (nove) aleatoriamente e solicita os FO
 - Envia os respectivos FO dos 9 (nove) escolhidos

- Protocolo de votação com assinatura cega
 - ICT
 - Verifica em sua base de dados que o votante não encaminhou mensagens para assinatura anteriormente
 - Abre os 9 (nove) conjuntos de mensagens escolhidos aleatoriamente e os verifica
 - Assina individualmente cada uma das mensagens do conjunto que ela não abriu
 - Envia o conjunto devidamente assinado ao votante, armazenando a identificação do votante em sua base de dados

- Protocolo de votação com assinatura cega
 - Votante
 - Remove o FO e abre o conjunto
 - Contém 1 (um) voto válido assinado pela ICT para cada candidato da eleição
 - Escolhe o seu voto (democracia !) e o encripta com a chave pública da ICT
 - Envia seu voto a ICT

Votação Eletrônica

- Protocolo de votação com assinatura cega
 - ICT
 - Decriptografa o voto
 - Verifica a assinatura
 - Verifica a base de dados contra duplicação do identificador da mensagem
 - Salva o identificador da mensagem e o respectivo voto
 - Contabiliza o voto
 - Publica o resultado da eleição ao final
 - Publica a lista de identificador da mensagem e voto para verificação de contabilização e adulteração

Votação Eletrônica

Votação Eletrônica

CEUB

EDUCAÇÃO SUPERIOR

- Votação com duas instalações centrais
 - Agência central de legitimação (ACL)
 - Instalação central de tabulação (ICT)
- Separar as instalações aumenta a segurança do protocolo no sentido que uma sabe a lista dos eleitores, e a outra sabe os votos
 - A segurança depende da garantia que elas não conversam entre si, mantendo suas bases de dados separadas

Votação Eletrônica

- Protocolo de votação com duas instalações centrais
 - Votante envia mensagem a ACL solicitando um número de validação
 - ACL
 - Envia número de validação randômico ao votante
 - Guarda a lista de números de validação gerados
 - Guarda a lista de votantes
 - Envia a lista de números de validação a ICT
 - Votante cria um número de identificação

- Protocolo de votação com duas instalações centrais
 - Votante cria uma mensagem com
 - Seu número de identificação
 - O número de validação recebido da ACL
 - Seu voto
 - Votante envia essa mensagem a ICT

Votação Eletrônica

- Protocolo de votação com duas instalações centrais
 - ICT
 - Verifica o número de validação com a lista enviada pela ACL
 - Caso o número não exista, ignora
 - Caso o número exista, salva o número de identificação e o respectivo voto
 - » Marca que o número de validação já foi utilizado
 - Publica a lista de números de identificação e voto para verificação de contabilização e adulteração

- Protocolo all-or-nothing disclosure of secrets (ANDOS)
 - Alice possui muitos segredos e esta vendendo
 - Bob quer comprar um segredo
 - Protocolo garante que quando Bob adquirir informação sobre algum dos segredos, ele gastou a única chance que tinha de adquirir informação sobre qualquer um dos outros segredos
 - Há vários protocolos ANDOS na literatura de criptografia
 - Há um muito simples com RSA

Votação Eletrônica

- Protocolo de votação com uma única ICT e ANDOS
 - ICT utiliza o protocolo ANDOS para distribuir números de validação anonimamente
 - Esse protocolo permite votações não obrigatórias além de permitir a alteração segura do voto durante o período de votação
 - Garante 6 (seis) dos 7 (sete) requisitos mínimos para votação eletrônica, menos o "todos os votantes têm a garantia de que seu voto foi contabilizado na tabulação final"

Votação Eletrônica

- Protocolo de votação sem ICT
 - Projetado por Michael Merritt
 - Tão pesado que não pode ser implementado pragmaticamente
 - Todos os votantes possuem um par de chaves pública e secreta
 - Todos os votantes sabem a chave pública de todos os outros
 - Cada voto, de cada votante, é encriptado com a chave pública de todos os outros votantes, de forma que todos são necessários para verificar o voto de cada um

Votação Eletrônica

CEUB

EDUCAÇÃO SUPERIOR

- Iniciativas no planeta
 - Bélgica (1999)
 - Australia (2001)
 - Índia (2004)
 - Estonia (2005)
 - Brasil (1996)

Votação Eletrônica

- Artigos
 - Pedro Rezende
 - Devagar com o andor da urna
 - <https://www.cic.unb.br/~pedro/trabs/penetracao.html>
 - Bruce Schneier
 - Securing Elections
 - https://www.schneier.com/blog/archives/2018/04/securing_electi_1.html
 - On Blockchain Voting (!)
 - <https://www.schneier.com/blog/archives/2020/11/on-blockchain-voting.html>

Urna Eletrônica Brasileira



- Microcomputador de uso específico para eleições
 - Resistente
 - Pequenas dimensões
 - Leve
 - Autonomia de energia
 - Recursos de segurança

- Histórico
 - Desenvolvimento em 1995
 - Instituto Nacional de Pesquisas Espaciais (INPE)
 - Centro Técnico Aeroespacial de São José dos Campos (CTA)
 - Primeira utilização em 1996

- Características
 - Solução universal
 - Aderência à legislação vigente
 - Processo amigável
 - Custo reduzido
 - Perenidade
 - Segurança (?)
 - Facilidade na logística
 - Autonomia

Urna Eletrônica Brasileira

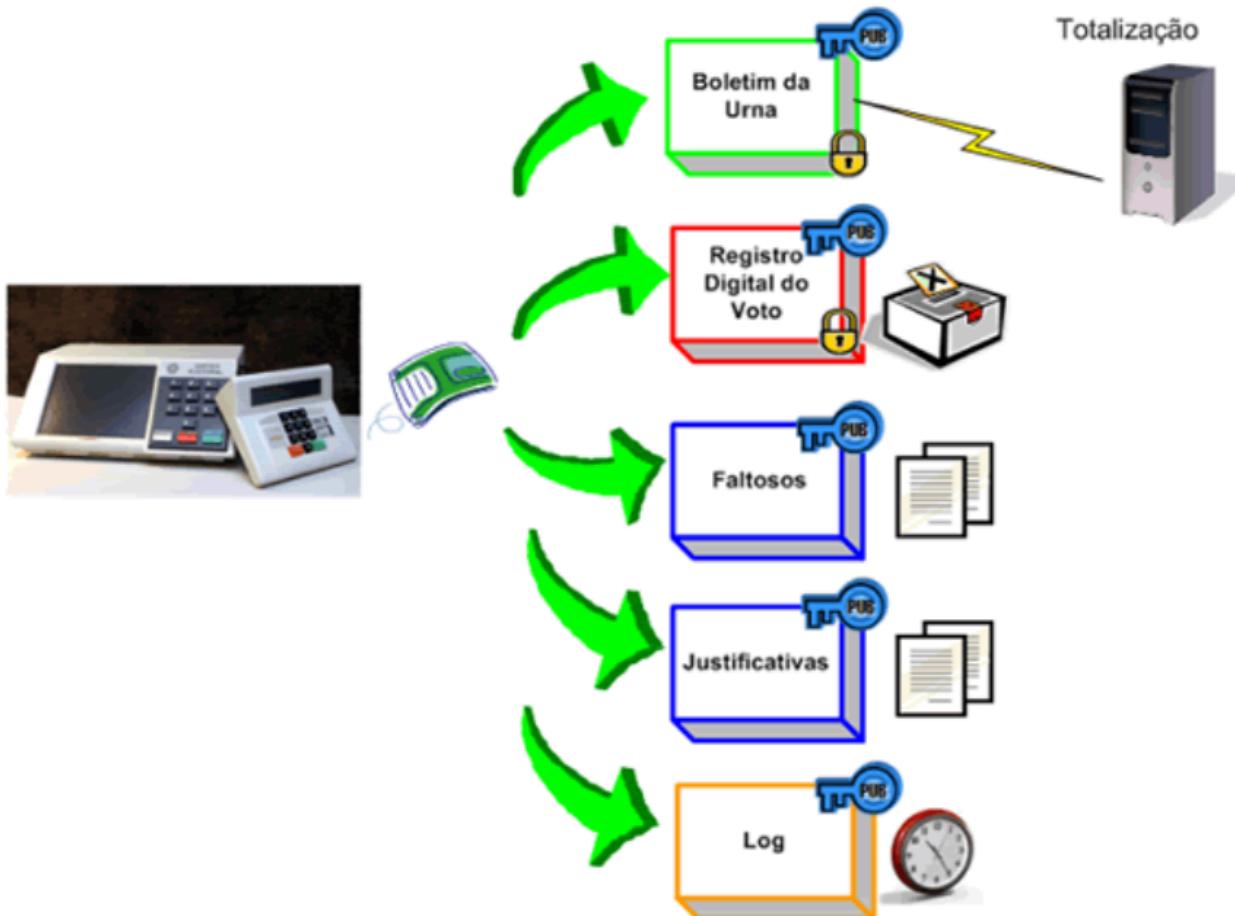
- Dois terminais compõem a urna eletrônica
 - Terminal do mesário
 - Terminal do eleitor



- Componentes
 - Memória de resultado
 - Impressora térmica
 - Cabos de alimentação
 - Bateria interna
 - Bateria externa
 - Memória flash
 - USB
 - Áudio para deficientes

Urna Eletrônica Brasileira

- Produtos gerados



- A urna eletrônica somente grava a indicação de que o eleitor já votou
- Pelo embaralhamento interno e outros mecanismos de segurança, não há nenhuma possibilidade de se verificar em quais candidatos um eleitor votou (?)

- Segurança
 - Assinatura digital
 - Garantir que a integridade de um conteúdo possa ser verificada
 - Garantir que o programa de computador não foi modificado de forma intencional
 - Garantir que o programa de computador não perdeu suas características originais por falha na gravação ou leitura
 - Se a assinatura digital for válida, o arquivo não foi modificado.
 - Assegurar a autenticidade do programa
 - Confirmar que o programa tem origem oficial e foi gerado pelo Tribunal Superior Eleitoral (TSE)

- Segurança
 - Resumo criptográfico (hash)
 - Calcular os hashes de todos os arquivos da urna
 - Publicar todos os resumos no portal do TSE

- Segurança
 - Sistema operacional específico Uenux
 - Hardware criptográfico
 - Isolamento de rede física e sem fio
 - Cerimônia de assinatura digital e lacração dos sistemas
 - Partidos políticos
 - Coligações
 - Ministério Público
 - Ordem dos Advogados do Brasil
 - Polícia Federal
 - Pessoas autorizadas em resolução específica

- Segurança
 - Lacre de segurança especial fabricado pela Casa da Moeda Brasileira
 - Zerésima
 - Boletim de urna ao final da eleição

- Auditorias
 - Unicamp em 2002
 - Polícia Federal em 2008 e 2018
 - Fundação de Apoio à Capacitação em Tecnologia da Informação (FACT)
 - Centro de Tecnologia da Informação Renato Archer

- Teste público de segurança
 - Objetiva contribuir para o aperfeiçoamento do software e do hardware da urna eletrônica
 - Demonstra a transparência do sistema
 - Investigadores inscritos apresentam e executam planos de ataque aos componentes externos e internos da urna eletrônica

- Teste público de segurança 2009
 - Sérgio Freitas da Silva
 - Obteve sucesso no ataque (!)
 - Demonstrar a interceptação da radiação eletromagnética emitida pelo teclado da urna eletrônica por meio de receptores de rádio específicos

- Teste público de segurança 2009
 - Carlos Eduardo Negrão de Oliveira (Tribunal Superior do Trabalho)
 - Não obteve sucesso no ataque
 - Demonstrar a alteração do boletim de urna substituindo a impressora da urna eletrônica

- Teste público de segurança 2009
 - Divailton Teixeira Machado (Superior Tribunal de Justiça)
 - Não obteve sucesso no ataque
 - Executar ataque de negação do serviço em uma determinada urna eletrônica
 - Quebrar o sigilo do voto por meio da análise de logs dos sistemas eleitorais

- Teste público de segurança 2009
 - Valter Monteiro Jr. (Marinha do Brasil)
 - Não obteve sucesso no ataque
 - Introduzir o código malicioso em mídias digitais na urna eletrônica ou em qualquer servidor do sistema de votação

- Teste público de segurança 2009
 - Thiago de Sá Cavalcanti (Polícia Federal)
 - Não obteve sucesso no ataque
 - Subverter a geração das mídias e o programa de votação

- Teste público de segurança 2009
 - Fernando Andrade Martins de Araujo (Controladoria Geral da União)
 - Obteve sucesso na avaliação (!)
 - Avaliar as vulnerabilidades das normas e dos procedimentos formais que disciplinam as eleições

- Teste público de segurança 2009
 - Antonio Gil Borges de Barros (Cáritas Informática Ltda)
 - Não obteve sucesso no ataque
 - Inserção de eleitores não cadastrados na seção para permitir o seu voto
 - Possibilitar a vinculação do eleitor ao seu voto
 - Porém conseguiu violar o lacre do envelope de transporte do flash de carga sem deixar vestígios facilmente perceptíveis (!)

- Teste público de segurança 2009
 - Nelson Murilo de Oliveira Rufino (Information Systems Security Association (ISSA))
 - Não obteve sucesso no ataque
 - Aplicar alteração nos arquivos de entrada de eleitores para manipular o resultado de uma eleição
 - Permitir que os eleitores cadastrados possam votar em duas ou mais seções diferentes

- Teste público de segurança 2009
 - Mauro César Sobrinho (Procuradoria Geral da República)
 - Não obteve sucesso no ataque
 - Substituir o núcleo do sistema operacional Linux da urna
 - Resgatar a chave pública contida no compact flash e reassinar todos os arquivos binários presentes na urna
 - Obteve sucesso na decifração, alteração e recifração do núcleo do sistema operacional (!)
 - Não conseguiu ultrapassar a etapa de validação do núcleo

- Teste público de segurança 2012
 - Diego de Freitas Aranha
 - Plano de ataque não realizado
 - Tentativa não rastreável de fraude no resultado da votação
 - Obteve sucesso no ataque (!)
 - Tentativa não rastreável de quebra de sigilo de votação

- Teste público de segurança 2012
 - Lauro Cesar Araujo
 - Plano de ataque não realizado
 - Quebra de sigilo do voto utilizando um aparelho celular
 - Fraude no sistema de apuração utilizado no exterior

- Teste público de segurança 2012
 - Marcelo Achar
 - Não obteve sucesso no ataque
 - Boot com loader não assinado
 - USB-Ethernet
 - Obteve sucesso no ataque (!)
 - Clonagem de memória flash de votação

- Teste público de segurança 2012
 - Luis Fernando de Almeida
 - Plano de ataque não realizado
 - Injeção de código e violação da rotina de aleatoriedade
 - Mapeamento de voto com o eleitor
 - Não obteve sucesso no ataque
 - Invalidação do flash card
 - Execução de shell code

- Teste público de segurança 2012
 - Marcelo Rodrigues de Sousa
 - Plano de ataque não realizado
 - Quebra do sigilo do voto eletrônico
 - Tentativa de comprometimento do MSD através da interface JTAG
 - Obteve sucesso no ataque (!)
 - Modificação do boot da urna
 - Tentativa de recuperação de dados da memória volátil do equipamento

- Teste público de segurança 2012
 - André Luiz Moura dos Santos
 - Não obteve sucesso no ataque
 - Teste de segurança do sistema eletrônico de votação do TSE

- Teste público de segurança 2012
 - Thiago de Sá Cavalcanti
 - Não obteve sucesso no ataque
 - Extração de dados da memória RAM da urna eletrônica

- Teste público de segurança 2012
 - Ricardo Antonio Pralon Santos
 - Não obteve sucesso no ataque
 - Teste de exploração dos mecanismos de proteção de carga da urna

- Teste público de segurança 2012
 - Suzana Brandt Dias
 - Plano de ataque não realizado
 - Comprometimento da transferência dos resultados obtidos nas urnas para o servidor do TRE/TSE

- Teste público de segurança 2016
 - André Henrique de Siqueira
 - Obteve sucesso no ataque (!)
 - Teste do sistema de apuração por votação totalmente eletrônica (boletim de urna)

- Teste público de segurança 2016
 - Charles Figueredo de Barros
 - Plano de ataque não realizado
 - Análise da segurança do armazenamento de arquivos e valores na memória da urna e nas mídias removíveis
 - Análise de práticas de programação relacionadas ao uso de primitivas criptográficas e outros aspectos de segurança do código fonte
 - Não obteve sucesso no ataque
 - Ataque ao sigilo do voto

- Teste público de segurança 2016
 - Elisabete Evaldt
 - Não obteve sucesso no ataque
 - Tentativa de fraude na destinação dos votos na urna através de controle dos dispositivos de teclado e impressora

- Teste público de segurança 2016
 - Luis Fernando de Almeida
 - Obteve sucesso no ataque (!)
 - Quebra do sigilo do voto baseado em gravação do áudio disponibilizado para pessoas com deficiência visual

Urna Eletrônica Brasileira

- Teste público de segurança 2016
 - João Felipe Souza
 - Não obteve sucesso no ataque
 - Registrador do teclado
 - Destruidor de votos
 - Rootkit JE connect
 - Obteve sucesso no ataque (!)
 - Reflash de urna

- Teste público de segurança 2016
 - Marcelo Muzili
 - Plano de ataque não realizado
 - Invasão no transporte dos dados no sistema de votação

- Teste público de segurança 2017
 - Cassio Goldschmidt
 - Obteve sucesso no ataque (!)
 - Revisão de código e teste dinâmico de geração das mídias para a preparação da urna eletrônica (GEDAI-EU)

- Teste público de segurança 2017
 - José Carlos Gama Quirino
 - Não obteve sucesso no ataque
 - Ataque aos sistemas dos hardwares e softwares da urna eletrônica

- Teste público de segurança 2017
 - Marcelo dos Anjos
 - Plano de ataque não realizado
 - Teste invasão hardware/software
 - Alteração de dados da votação

- Teste público de segurança 2017
 - Rodrigo Cardoso Silva
 - Não obteve sucesso no ataque
 - Programa Transportador de Arquivos – “teste Doodle”
 - Uinux e softwares básicos Metamorfose (Kafka)

- Teste público de segurança 2017
 - Diego de Freitas Aranha
 - Plano de ataque não realizado
 - Execução remota de código na plataforma web
 - Tentativa de violação do sigilo do voto
 - Inserção de dispositivo USB malicioso
 - Obteve sucesso no ataque (!)
 - Capturar a chave secreta da urna eletrônica, por meio de ataques ao cartão de memória utilizado para fazer carga nas urnas
 - Execução de código estranho de impressão na urna eletrônica
 - Violiação de sigilo de voto individual sensível
 - Violação da integridade do software de votação

- Teste público de segurança 2017
 - Luis Antonio Brasil Kowada
 - Não obteve sucesso no ataque
 - Análise do uso dos procedimentos criptográficos

- Teste público de segurança 2017
 - Ivo de Carvalho Peixinho
 - Obteve sucesso no ataque (!)
 - Executar o software da urna eletrônica em um computador e, a partir daí, tentar extrair a chave secreta da urna eletrônica

- Teste público de segurança 2019
 - Fellipe Ribeiro Silva Abib
 - Não obteve sucesso no ataque
 - Identificação do eleitor e de seu voto a partir das informações gravadas no Registro Digital do Voto (RDV) e tentativa de manipulação do Boletim de Urna (BU)

- Teste público de segurança 2019
 - Jairo Simão Santana Melo
 - Não obteve sucesso no ataque
 - Identificação da operação eletrônica da urna, analisando os sinais elétricos nos circuitos entre o teclado e a placa mãe, empregando técnicas de inteligência artificial para identificação de cada tecla pressionada

- Teste público de segurança 2019
 - Luis Antonio Brasil Kowada
 - Não obteve sucesso no ataque
 - Obtenção de chaves criptográficas e verificação do correto uso da criptografia para a garantia da integridade, confidencialidade e autenticidade
 - Verificar a proteção de programas pré-construídos (denominados de bibliotecas), necessários ao sistema da urna

- Teste público de segurança 2019
 - Luís Fernando de Almeida
 - Não obteve sucesso no ataque
 - Tentativa de uso de Machine Learning para reproduzir o padrão de geração dos números aleatórios e, consequentemente, comprometer o sigilo do voto

- Teste público de segurança 2019
 - Paulo César Herrmann Wanner
 - Plano de ataque não realizado
 - Domínio do sistema de geração de mídia a fim de adulterar dados de preparação da urna da seção eleitoral
 - Obteve sucesso no ataque (!)
 - Recuperação de senhas de acesso dos sistemas de transmissão do Boletim de Urna para enviar votos falsos
 - Quebra da criptografia da proteção (SIS) do sistema gerador de mídia das urnas eletrônicas (GEDAI)

- Teste público de segurança 2019
 - José Fellipe de Moraes Albano
 - Não obteve sucesso no ataque
 - Identificação de componentes da rede computacional do TSE de forma a identificar possíveis alvos e disparar ataques específicos contra serviços disponibilizados na rede

- Teste público de segurança 2019
 - Leonardo Cunha dos Santos
 - Não obteve sucesso no ataque
 - Quebra do sigilo do voto por meio de detecção de padrões de comportamento elétrico durante o pressionamento de teclas

!! Obrigado !!

ceub.br

