

Segurança

em

Sistemas de Informação

Sumário

1. Introdução
2. Segurança
 - Conceitos Básicos
 - Estratégias
 - As 3 faces da Segurança
3. Segurança Lógica
 - Abrangência
 - O Contexto Criptológico
 - Uma implementação
4. Perspectivas
5. Conclusão

Ao autor de uma história toca aprofundar tudo, dissertar sobre tudo, procurar todos os detalhes; mas o que resume deve, ao contrário, procurar condensar a narrativa e evitar a minúcia na exposição dos fatos.

(II - Macabeus, 2 : 30, 31)

1. Introdução

Sistemas de Informação (S.I.)

Sistemas baseados em (HW, SW, PW) para tratamento da informação

Tratamento = { captura, validação, armazenamento, recuperação, transmissão e manipulação }

Segurança

Proteção contra { Destruição
Vazamento
Modificação { Intencional
Acidental } } da Informação

e mau uso dos recursos

2. Segurança

2.1. Conceitos Básicos

i) Sistema de Informação Seguro

5 características: {

- Disponibilidade
- Integridade
- Confidencialidade
- Autenticação
- Não repúdio

(IS 7498-2 NIST)

ii) Custos: {

- R\$
- Overhead

2. Segurança (cont.)

2.2. Estratégias

i) NAS (Network Attached Storage)

Armazenamento, backup e restauração “Self-made”.

ii) SAN (Storage Area Network)

2.3. As 3 faces da Segurança:

Operacional

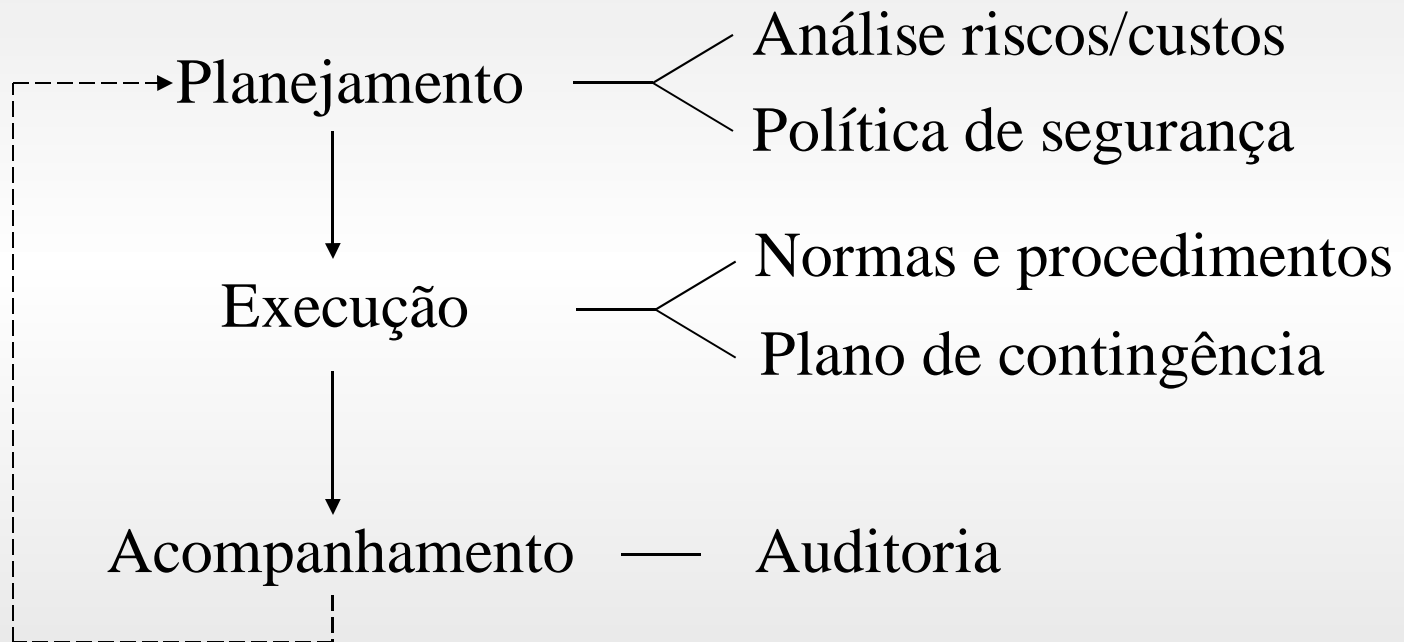
Física

Lógica

2. Segurança (cont.)

i) Segurança Operacional

(Ciclo da administração da Segurança)



A NBR/ISO 17799

- As BS 5750 (1979)
- As BS 7799
- A ISO 17799: estabelece, em 10 capítulos, um referencial para desenvolver, implementar e avaliar a **Gestão** da Segurança da Informação.
- Válida desde 30/9/2001

2. Segurança (cont.)

ii) Segurança Física

Controles {
Acesso (Biometria *)
Condições ambientais
Imprevistos

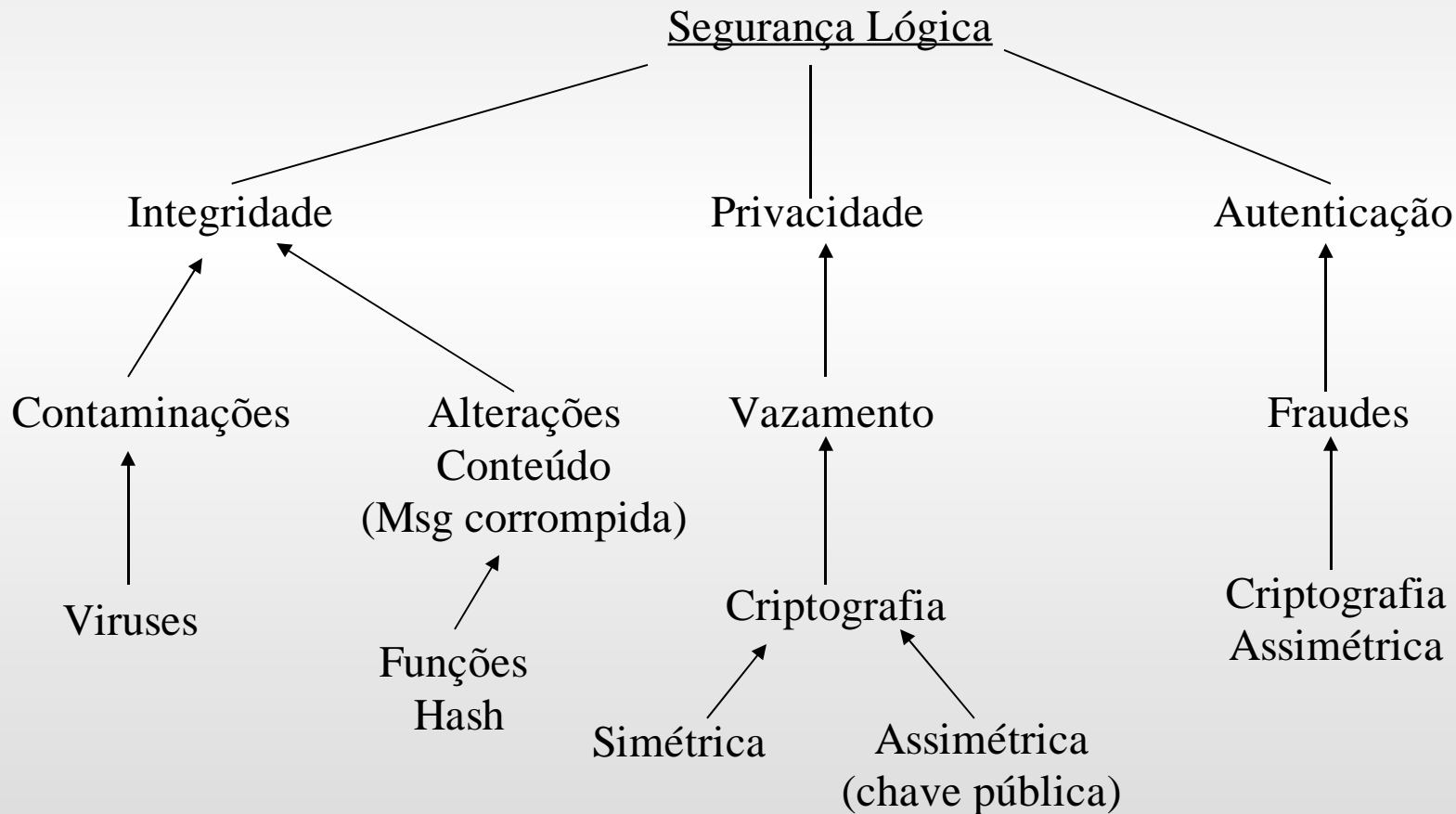
(*) <http://www.iriscan.com>

<http://www.identix.com>

<http://www.voice-security.com>

3. Segurança Lógica

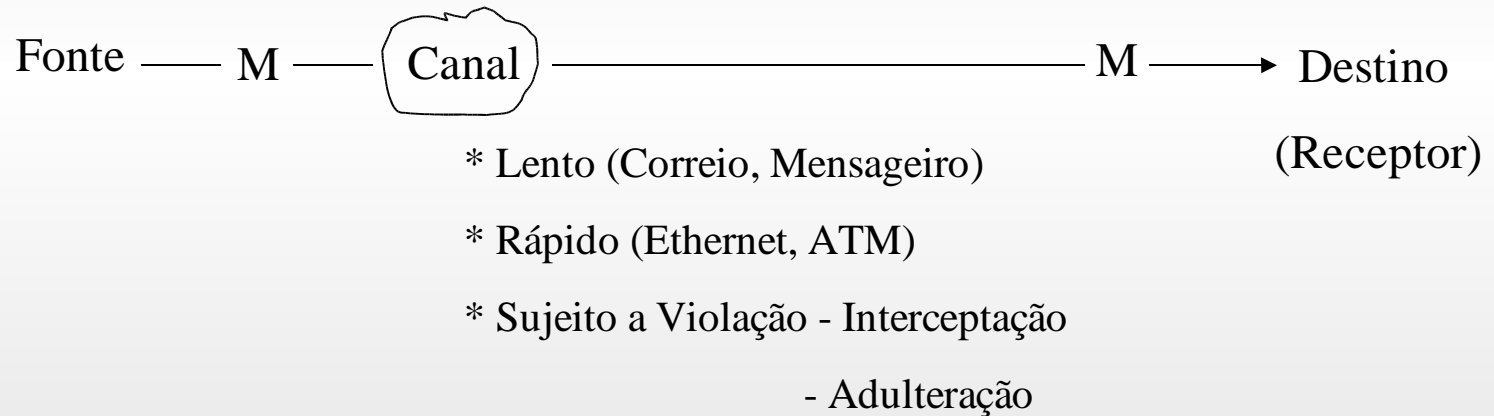
3.1. Abrangência



3. Segurança Lógica (Cont.)

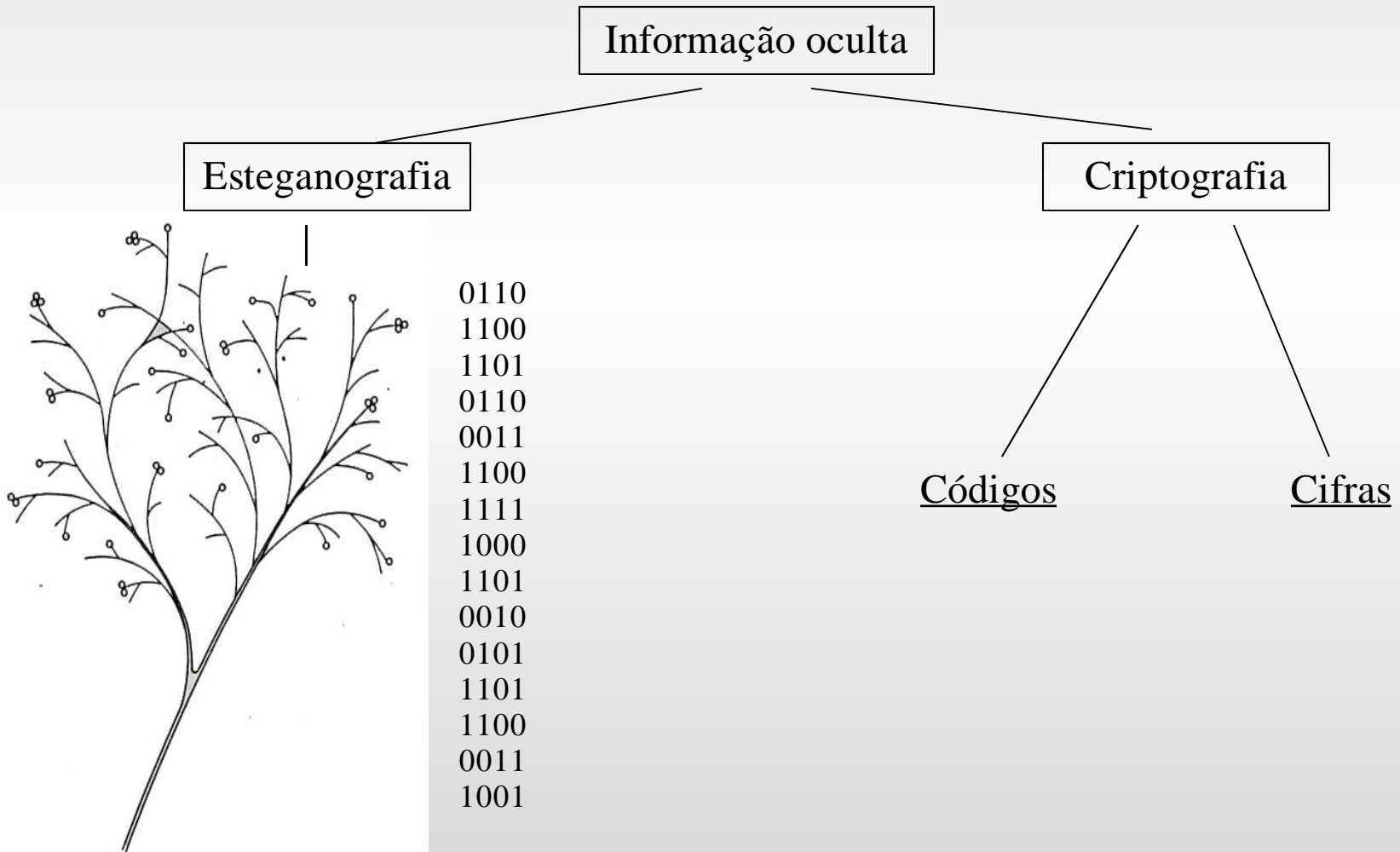
3.2. O Contexto Criptológico

i) Generalidades



3. Segurança Lógica (Cont.)

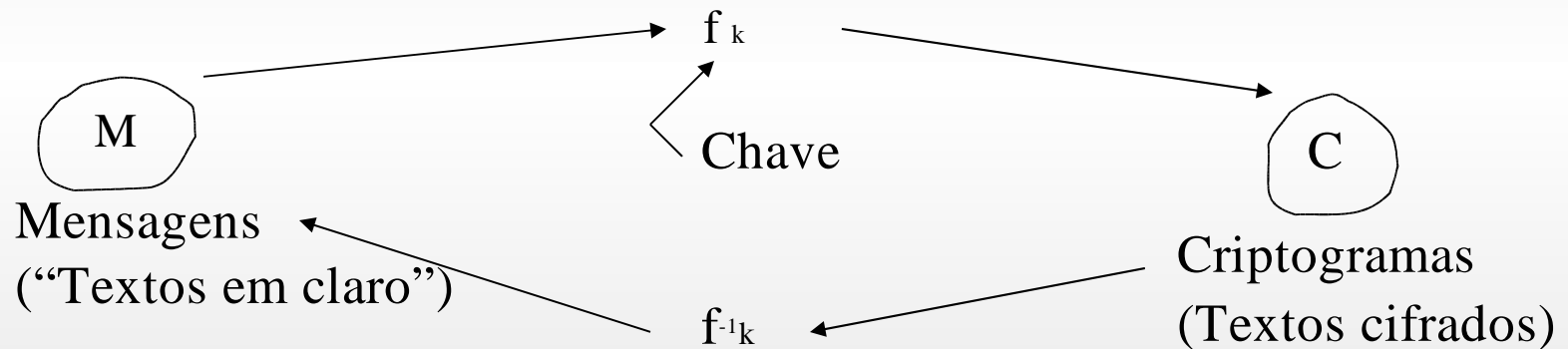
ii) Criptologia



3. Segurança Lógica (Cont.)

iii) Criptografia

Técnicas para assegurar sigilo e autenticação do conteúdo da mensagem



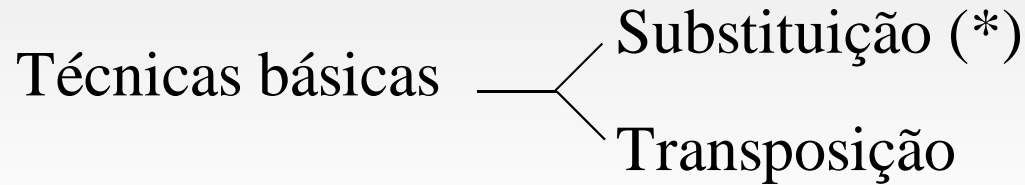
$$C = f_k (M)$$

$$M = f_k^{-1} (C) = f_k^{-1} (f_k (M)) = M$$

3. Segurança Lógica (Cont.)

3.3. Criptografia

i) Criptografia Clássica



(*) HAL

$\#K = 25! \cong 50.000 * \text{idade da Terra}$

AEOSN

3. Segurança Lógica (Cont.)

ii) Shannon

Transformação misturadora

D.U. = Quantidade mínima de texto cifrado que permite solução única

$$N = H(K) / D$$

Entropia da chave

Redundância do idioma

A cifra inquebrável

3. Segurança Lógica (Cont.)

iii) O DES

- 1972: NBS e NSA buscam um padrão
- 1973/74: Convites à Comunidade Científica
Feistel e o Lúçifer
A Solução IBM
- 1975: implementação em chip LSI
- Transformação misturadora
- Blocos de 64 bits com chave de 56 bits
- 1976: A Polêmica

DIFFIE & HELLMAN: CHAVE CURTA

(Criptoanálise p/ exaustão)

- 1977/78: 2 seminários
Hardware: DES ok p/ 15 anos
- Adotado pelos EUA para dados não classificados (1977)

3. Segurança Lógica (Cont.)

- O **AES**
- **1997 = chamada do NIST para seleção do padrão substituto do DES para as 3 primeiras décadas do século XXI**
- **1999 = 5 selecionados;**
- **2000 = algoritmo RIJNDAEL escolhido como AES**
- **Algoritmo de criptografia simétrica com chaves de 128 a 256 bits. Como não utiliza estrutura de Feistel, é enxuto e rápido, apesar de operar com multiplicações polinomiais sobre GF (2)**
- **Utilizado mesmo com recursos computacionais escassos (celulares e smartcards)**

3. Segurança Lógica (Cont.)

iv) Criptografia Simétrica (Limitações)

O problema da logística da distribuição das chaves

Para uma rede de n nós, há a necessidade de:

$$n * (n-1) / 2 \quad \text{canais seguros}$$

Ex: Para rede de 100 nós \approx 4950 canais seguros (!!!)

3. Segurança Lógica (Cont.)

v) Criptografia Assimétrica

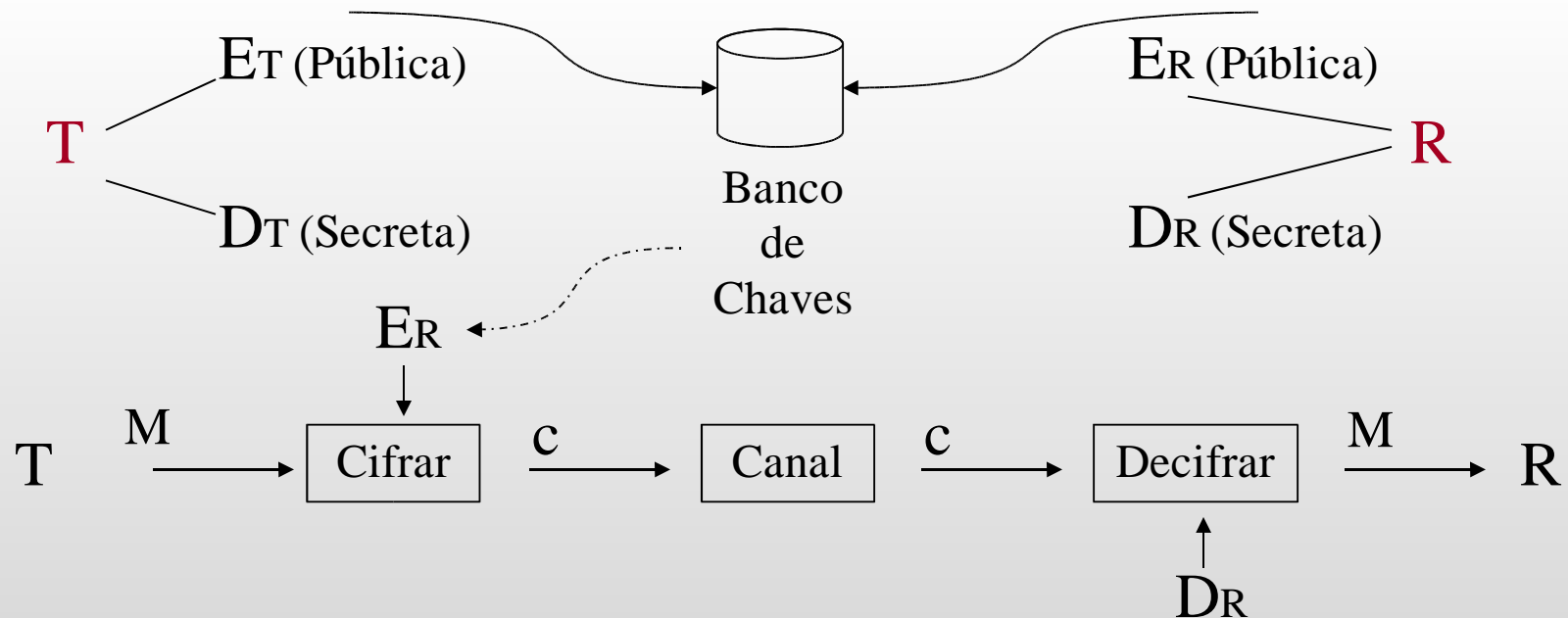
- 1973: Diffie e Hellmann

Uso de funções “One-way”

Solução para o problema da Logística das chaves

Bônus: Assinatura Digital

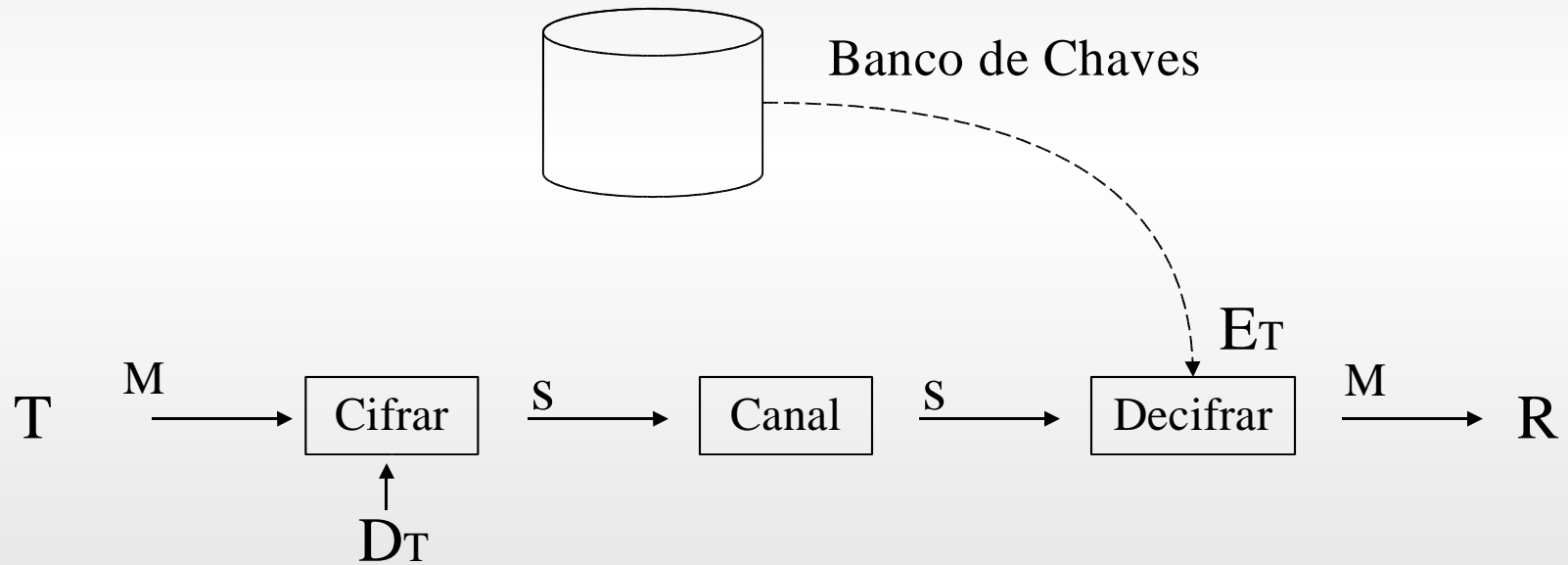
- Visão do Processo



3. Segurança Lógica (Cont.)

Assinatura Digital

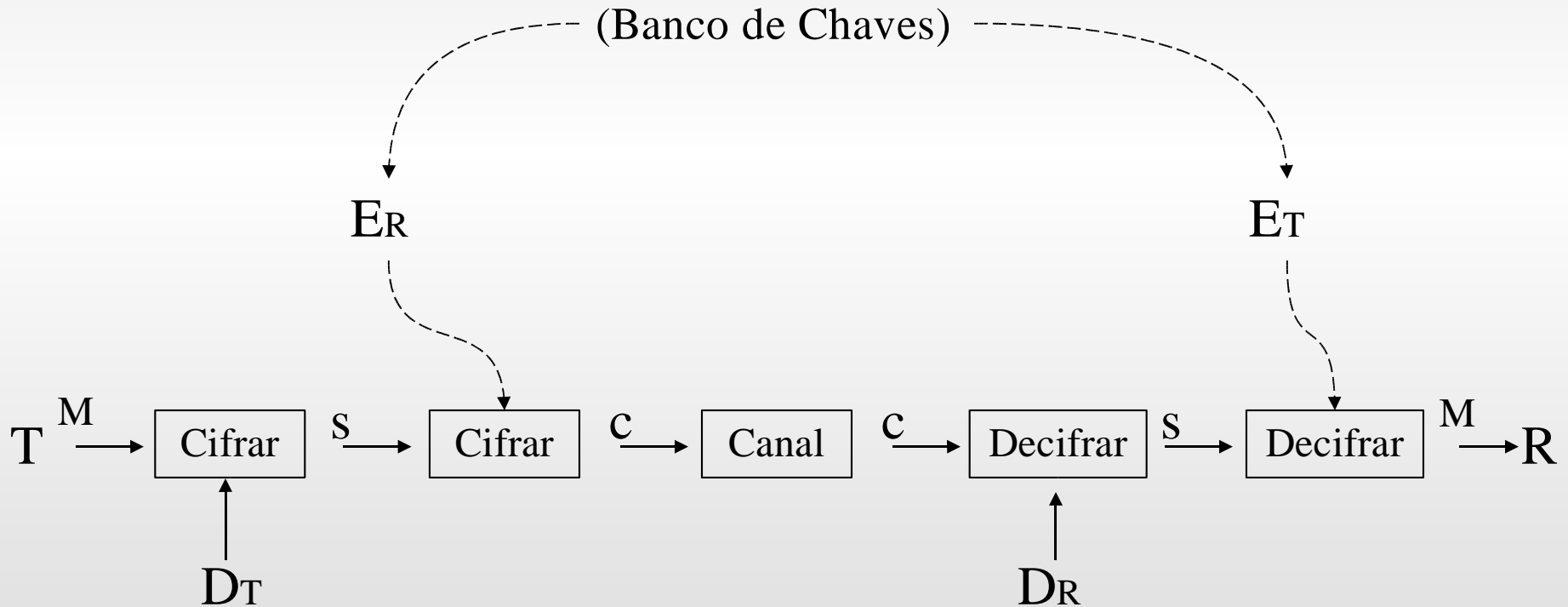
Sem Sigilo



3. Segurança Lógica (Cont.)

Assinatura Digital

Com Sigilo



3. Segurança Lógica (Cont.)

- Funções “One-Way”

$$\text{Ex.: } \left\{ \begin{array}{l} \text{Fatorar } 29.083 (?) \\ \text{Multiplicar } 127 \times 229 = 29.083 \end{array} \right.$$

- Fatoração de alguns n^{os} $\left\{ \begin{array}{l} \text{Problema intratável} \\ \text{Computacionalmente inviável} \end{array} \right.$

- Tipos Desses n^{os} :

$$\text{Fermat: } 2^{2^n} + 1$$

$$N = (p \cdot q) = p, q \text{ primos muito grandes}$$

- Melhor algoritmo de fatoração (Schroeppel)

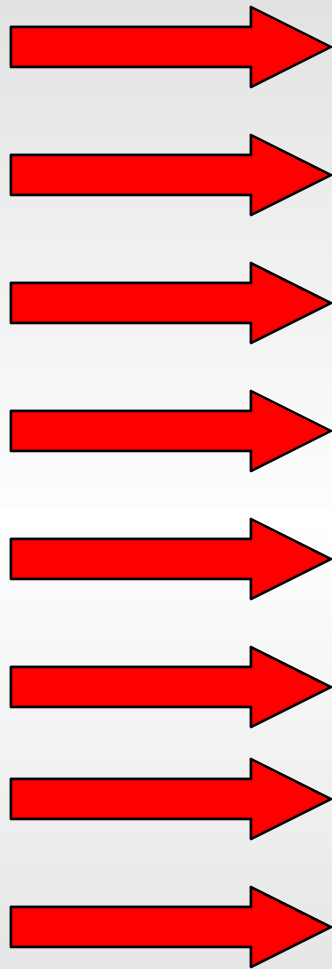
74 anos para fatorar N com 100 algarismos

- Segredos de estado produtos de números primos grandes

3. Segurança Lógica (Cont.)

3.4. Uma implementação

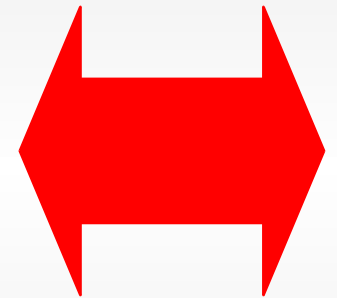


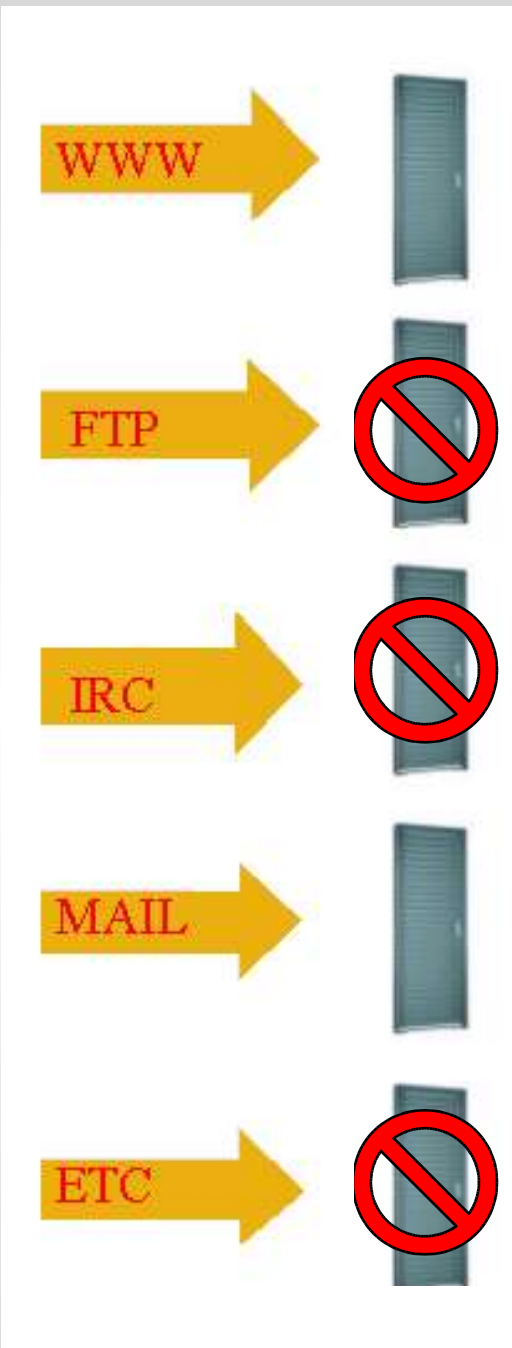


INTERNET

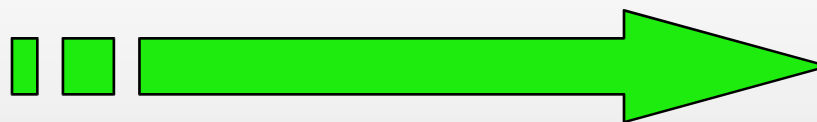


**REDE
INTERNA**



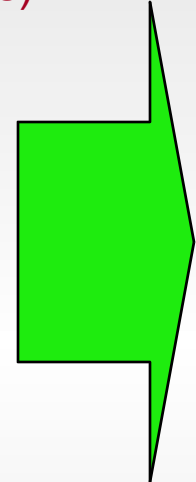
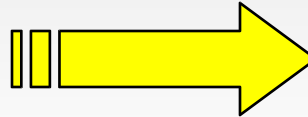


**SELECIONA QUAIS
PORTAS FICARÃO
ABERTAS**



SURFINGATE
(Finjan)

MIMESWEEPER
(Content Technologies)



Códigos
escondidos
em páginas
inocentes

Controle
de
conteúdos

4. Perspectivas

i) Humanístico/Gestão

- Ética
 - Psicologia
 - Jurídico
- ⇒ Auditorias

ii) Técnico

- Biometria
- Cartórios Digitais
- Banda Larga
- Wireless sobre spread spectrum

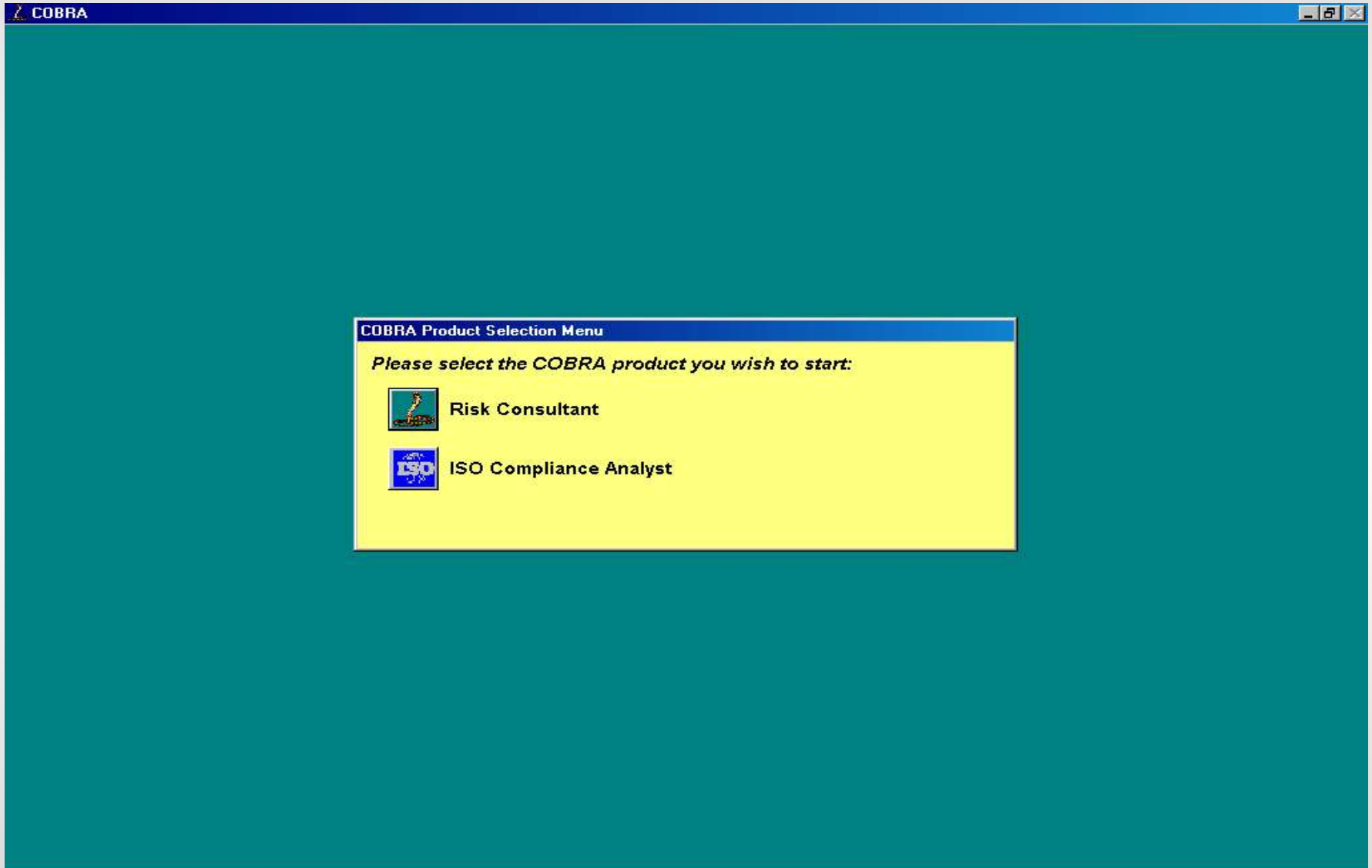
Softwares de Auditoria

(Exemplo: COBRA)

Em <http://www.securitypolicy.co.uk/bs-7799>

- Ferramenta Modular (2 Módulos);
- Risk Consultant
- ISO Compliance Analyst
- Baseada em questionários (módulos)
- Geração de Relatórios/Documentação

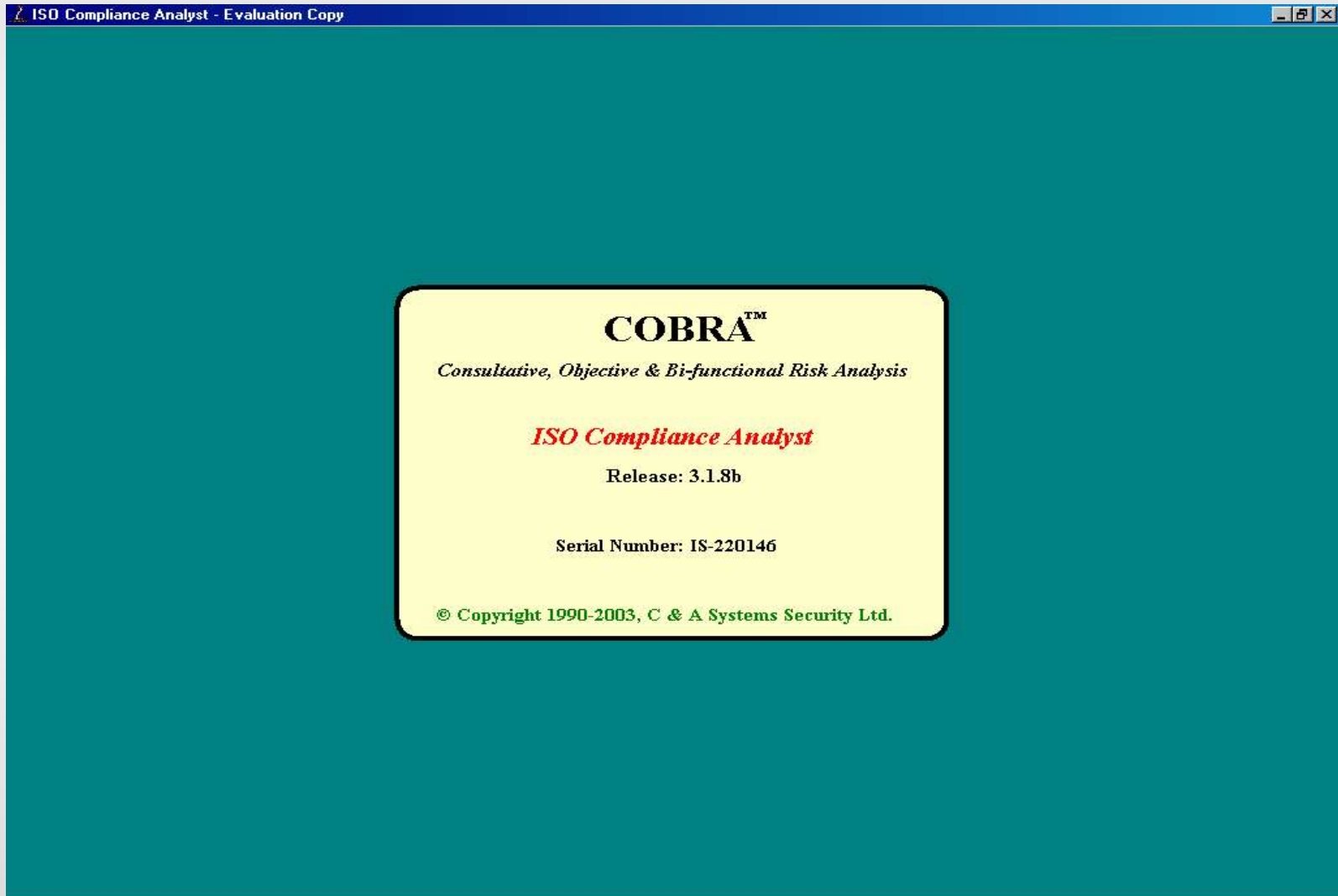
Tela Inicial



Opção Risk Consultant



Opção ISO Compliance Analyst



4. Perspectivas

i) Humanístico/Gestão

- Ética
 - Psicologia
 - Jurídico
- ⇒ Auditorias

ii) Técnico

- **Esteganografia**
- Cartórios Digitais
- Banda Larga
- Wireless sobre spread spectrum



Sob luz ultravioleta, a metade esquerda da nota mostra o valor em tom escuro e o rosto claro e fluorescente. A metade direita mostra o valor da nota em tom claro e fluorescente e o rosto em tom escuro.



Nas duas faces da nota um texto curto sobre a pessoa retratada é reproduzido numa impressão tão miniaturizada que, só com o auxílio de uma poderosa lente de aumento, é possível lê-lo.

O exemplo aqui reproduzido corresponde ao texto encontrado na frente da nota de 50 francos.

0DAS0UNIVERSEL0SCHAFFEN0000
0VON0SOPHIE0TAEUBER-ARPO00000
0UMFASST0DIE0BEREICHE0MALEREI0
0TEXTIL0PLASTIK0UND0RELIEF0000
0TANZ0THEATER0UND0MARIONET00
0TEN0SIND0IHRE0WEITEREN0ALS0
0DRUCKSMITTEL000ALS0GESTALTERIN0
0GIBT0SIE0WICHTIGE0IMPULSE0FUR0
0DIE0ENTWICKLUNG0DER0KON-000
0STRUKTIVEN0KUNST000000000000
0L'0VRA0UNIVERSALA0DA0SOPHIE0
0TAEUBER-ARPO0CUMPIGLIA000000
0PICTURA0TEXTILIAS0SCULPTURA00
0E0RE0LIEV000SAUT0TEATER0EMA0
0RIONETTAS0ENC0SES0ULTERIURS00
0MEDS0D'0EXPRESSION00000000000
0SCO0CREADRA0DAT0ELLA0IMPULSO
0IMPURTANTS0PER0IL0SVILUP0DA0
0L'0ART0CONSTRUCTIV000000000000

4. Perspectivas

i) Humanístico/Gestão

- Ética
 - Psicologia
 - Jurídico
- ⇒ Auditorias

ii) Técnico

- Biometria
- Cartórios Digitais
- Banda Larga
- **Wireless sobre spread spectrum**

Hedy Lamarr, inventor, has influenced, impacted, and changed Science and Technology. Her *spread spectrum technology* invention catalyzed a wireless revolution.

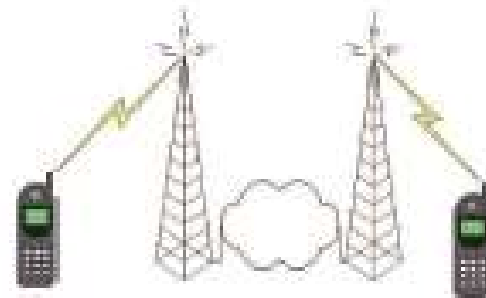


- **Nova tecnologia de redes sem fio**

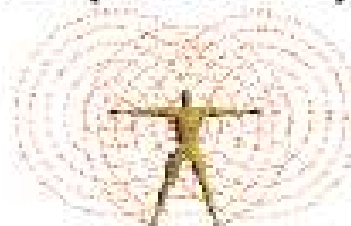
- **Novos problemas e necessidades**
- **Protocolos e sistemas antigos foram desenvolvidos considerando enlace com fios**
- **Necessidade de novo modo de pensamento para novos sistemas e meios de utilizar sistemas antigos**

Tipos de Redes Sem Fio

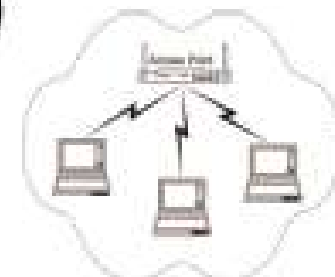
- **Telefonia móvel**
 - GSM / GPRS / 3G ...



- **Redes Pessoais sem Fio (WPAN)**
 - Bluetooth (IEEE 802.15)



- **Redes Locais sem Fio (WLAN)**
 - IEEE 802.11



Padrões 802.11

| Padrão IEEE | Velocidade | Frequência |
|-------------|---------------------|------------|
| 802.11 | 1 Mbps 2 Mbps | 2.4 GHz |
| 802.11a | Acima de 54 Mbps | 5 GHz |
| 802.11b | 5.5 Mbps 11 Mbps | 2.4 GHz |
| 802.11g | Acima de 54 Mbps | 2.4 GHz |

Segurança - WEP

- Criptografia simétrica
- XOR entre mensagem e chave
- Necessita de chave de mesmo tamanho da mensagem
 - Utiliza gerador de números pseudo-aleatórios do RC4 (PRNG)
 - utilizando um segredo como semente, cria uma chave do tamanho da mensagem

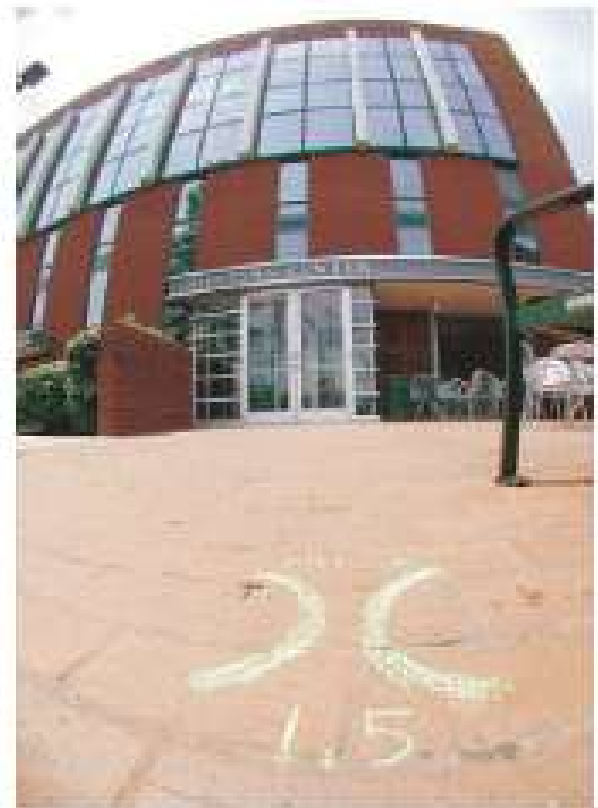
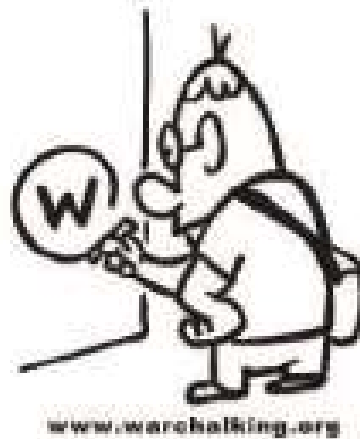
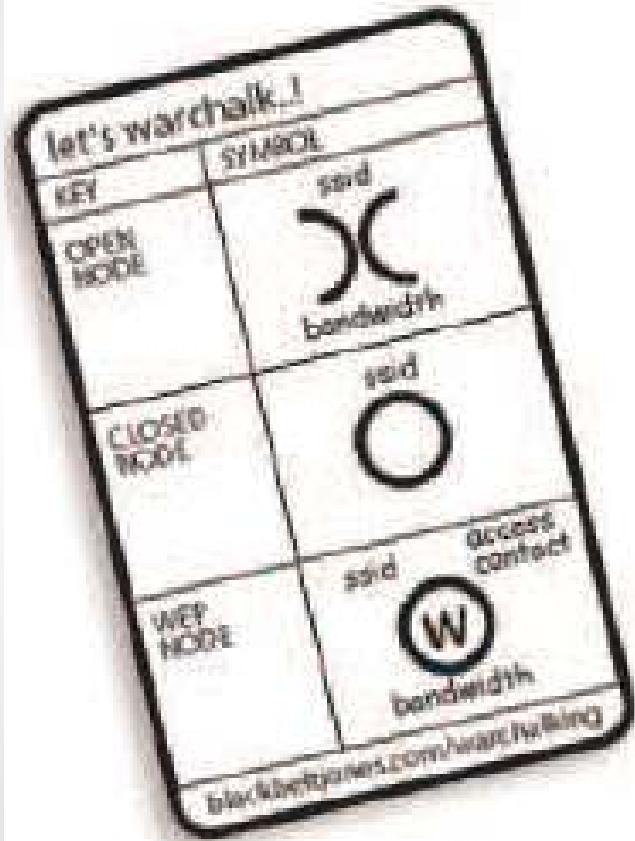
War Driving

- Os problemas do padrão motivaram o “estudo” das redes sem fio por “curiosos”
 - Desenvolvimento de antenas
 - Wardriving
 - Warchalking
 - Ferramentas

- **Kit para Wardriving:**



Warchalking



"Any girl can be glamorous. All she has to do is stand still and look stupid." -- Hedy Lamarr



4. Perspectivas (cont.)

iii) Alternativas à RSA

1988

400 computadores em conjunto

1 mês

9 412 343 607 359 262 946 971
172 136 294 514 357 528 981
378 983 082 541 347 532 211
942 640 121 301 590 698 634
089 611 468 911 681 =

= (86 759 222 313 428 390 812 218
077 095 850 708 048 917) *

* (108 488 104 853 637 470 612
961 399 842 972 948 409 834
611 525 790 577 216 753)

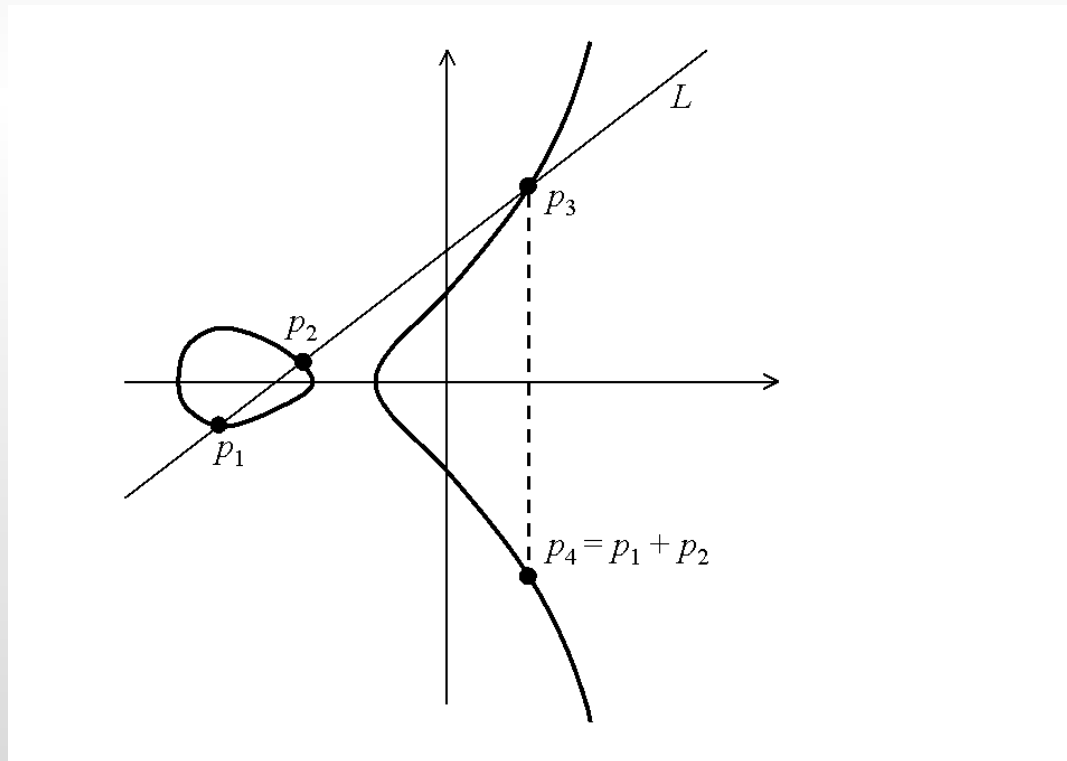
4. Perspectivas (cont.)

ECC (Elliptic Curve Cryptography)

$$y^2 = x^3 + ax + b$$

Dados L e $p_3 = (x, y)$

Determinar p_1 e $p_2 \mid p_4 = p_1 + p_2 \quad \wedge \quad p_4 = (x, -y)$



Conclusão

Encarregado por Segurança precavido:

1) Plano de Segurança

- (1) Política de segurança
- (2) Normas administrativas (RH, RM)
- (3) Procedimentos de Segurança Física, HW, Telecom
- (4) Procedimentos de segurança de SW
- (5) Procedimentos de Testes / Auditorias
- (6) Plano de contingência

2) Esquema de proteção Internet

3) RH treinado e motivado

Se você conhecer o inimigo e a si próprio, não precisará temer o resultado de cem batalhas. Se você se conhecer, mas não ao inimigo, para cada vitória conseguida também haverá uma derrota. Se você não conhecer o inimigo nem a si próprio, sucumbirá em todas as batalhas.

(Sun Tzu)

Segurança

em

Sistemas de Informação