Criptografi a

A Arte dos Segredos e da Confi ança

José Manuel E. Valença

Departamento de Informática, Universidade do Minho

Workshop SINO 2005 – Covilhã 7/Nov/2005

Conteúdo

Sociedade da Informação

- Existe um sistema social que é originário e motivado pelas **Tecnologias da Informação** (TI’s) e que, à falta de melhor nome, designamos por **Sociedade da Informação**.
- Como realidade social a dita “Sociedade de Informação” determina contextos sociais e relações entre contextos, a que genericamente chamamos **Sistemas de Informação**, que evoluem e se defi nem de uma forma que (penso) está longe da capacidade decisória de qualquer política.
- A Sociedade da Informação evolui metabólicamente condicionada por **tendências ecológicas** específi cas e que podem (por simplicidade) ser agrupadas em três dimensões:

Sociedade da Informação. . .

ubiquidade as TI’s “invadem” todas as facetas da actividade humana;
argumento subjacente: **eficácia**.

mobilidade aproveitamento limite de recursos computacionais escassos e fi sicamente condicionados; a evolução dos si’s para fora dos seus suportes físicos e para a essência da **informação pura**;
argumento subjacente: **democraticidade**.

hostilidade os si’s não são benignos: prevalece a competição e o conflito na SI; os direitos são uma questão essencial.
argumento subjacente: **segurança**

. . . à parte. . .

- *Ecologia* e *Economia* têm a mesma raiz (o vocábulo grego **oîkos** – casa) e sufi xos **logos** (linguagem, discurso) e **nomos** (norma, direcção, ordem); etimologicamente signifi cam, respectivamente, “a linguagem da casa” e “a norma da casa”.
- faz sentido falar de Ecologia da Informação (**infoecologia**) como

  estudo das relações dos agentes humanos ou artificiais entre si e entre o contexto (meio, ambiente, casa) informativo onde residem,

- como falar de Economia da Informação (**infoeconomia**) visto como

  estudo dos recursos, e dos fenómenos que geram e consomem tais recursos, necessários à evolução e sobrevivência do contexto informativo.

Hostilidade e Segurança

Na Sociedade da Informação a questão da garantia de direitos coloca-se quando a hostilidade é uma tendência prevalecente; o entendimento que se tenha desta hostilidade condiciona a perspectiva que se vai ter da *segurança*.

São possíveis dois pontos de vista: a perspectiva dita **determinística** e a perspectiva **caótica**.

Perspectiva Determinística a hostilidade é excepcional e indesejável

- a segurança é um atributo próprio de cada sistema de informação,
- quando a segurança é garantida por tecnologia (i.e. criptografi a) essa solução é parte integrante do sistema de informação e cumpre-lhe isolar o sistema de eventuais violações á sua funcionalidade e integridade.

*a segurança é **orientada ao sistema**; assume que existe uma fronteira nítida entre sistema e ambiente e uma eficiente caracterização de ambos; o papel da segurança é a preservação dessa funcionalidade; conduz naturalmente á conclusão que sistemas fechados são eminentemente mais seguros que sistemas abertos.*

Perspectiva Caótica: a hostilidade é prevalecente, natural e real.

- a segurança é a garantia dos direitos pessoais de cada agente num eco-sistema de si’s em constante competição e conflito,
- a tecnologia é “pessoal e democrática”: i.e. age ao nível das relações individuais dos agentes.

*a segurança é **orientada à confiança**; a fronteira entre sistema e ambiente é fluída e, por isso, só faz sentido falar de agentes, das suas relações e dos seus direitos; a noção de sistema de informação deve ser revista: pode ser apenas uma abstracção para um arranjo de relações inter-agentes; neste ponto de vista (algo extremo) os sistemas fechados, seguros ou não, nem sequer fazem sentido.*

Exemplo: o problema da “identifi cação”

A distinção entre perspectivas de segurança conduz a diferentes interpretações do papel atribuído aos utentes no acesso ao sistema acesso e do tipo de tecnologia usada no controlo desse acesso.

Num sistema de **home banking** uma perspectiva determinística da segurança preocupa-se em que nenhum utilizador viole a integridade do sistema e, dessa forma, a sua funcionalidade.
Uma perspectiva caótica teria tendência a privilegiar o equilíbrio de direitos entre o banco e os seus utentes assumindo que existem “interesses justos”, eventualmente em conflito, de ambos as partes.

Num **sistema de saúde** as duas perspectivas de segurança entram em evidente conflito: a preservação da funcionalidade ou integridade estão longe de ser sufi ciente para garantir os direitos de privacidade e confi dencialidade essenciais ao utente já que a hostilidade essencial é, frequentemente, interna ao sistema.

Os **tribunais** passaram a usar intensivamente as TI’s não só para estabelecer relações de cooperação entre agentes judiciais mas também para comunicar com outras instituições (escritórios de advocacia, outros tribunais, conservatórias, etc.).

Uma perspectiva determinística da segurança tende a concentrar-se na preservação da funcionalidade e integridade do sistema de informação do tribunal.

A perspectiva caótica tem a atenção os direitos que regulam as relações de confi ança entre os vários agentes intervenientes.

Criptografi a: a Arte

do livro “Modern Criptography, Probabilistic Proofs and Pseudo-Randomness” de O. Goldreich

Whereas classical criptography was confined to the art of designing and breaking encryption schemes (or “secrecy codes”) modern criptography is concerned with the rigorous analysis of any system which should withstand malicious attempts to abuse it.

We emphasize two aspects of transition from classical to modern criptography: (1) the widenning of scope from one specific task to an utmost wide general class of tasks; (2) the move from an enginnering-art which strives on ad-hoc tricks to a scientific discipline based on rigorous approaches and techniques.

Uma distinção limitativa e insufi ciente porque (penso)

- “Arte” não é contraponto de “rigor científi co”
  A Criptografia continua a ser uma “arte”, devidamente equipada com as ferramentas formais adequadas, mas uma arte ainda assim porque assenta numa sensibilidade muito específica sobre arranjos (frequentemente complexos, sub-especificados e ambíguos) de relações, direitos e ética na sociedade da informação.
- A natureza da “análise rigorosa” é deixada em claro.
  Qual é a natureza essencial da criptografia moderna que necessita de uma análise rigorosa? a complexidade computacional para atacar as técnicas criptográficas? a entropia informativa (chaves secretas, técnicas obscuras, . . .) ou algo ainda mais complexo? qual o papel da comunidade?

O que é “Criptografi a”?

Definição “tecnológica”

Criptografi a é a *tecnologia* para garantir a segurança dos sistemas de informação.

Definição “construtiva” (*Doldreich et al.*)

Criptografi a é a *disciplina* que lida com a construção de esquemas que resistam às tentativas hostis de os desviar de uma funcionalidade pré-estabelecida.

Definição “analítica”

Criptografi a é a *arte* dos segredos e da confi ança.

Uma “arte”?

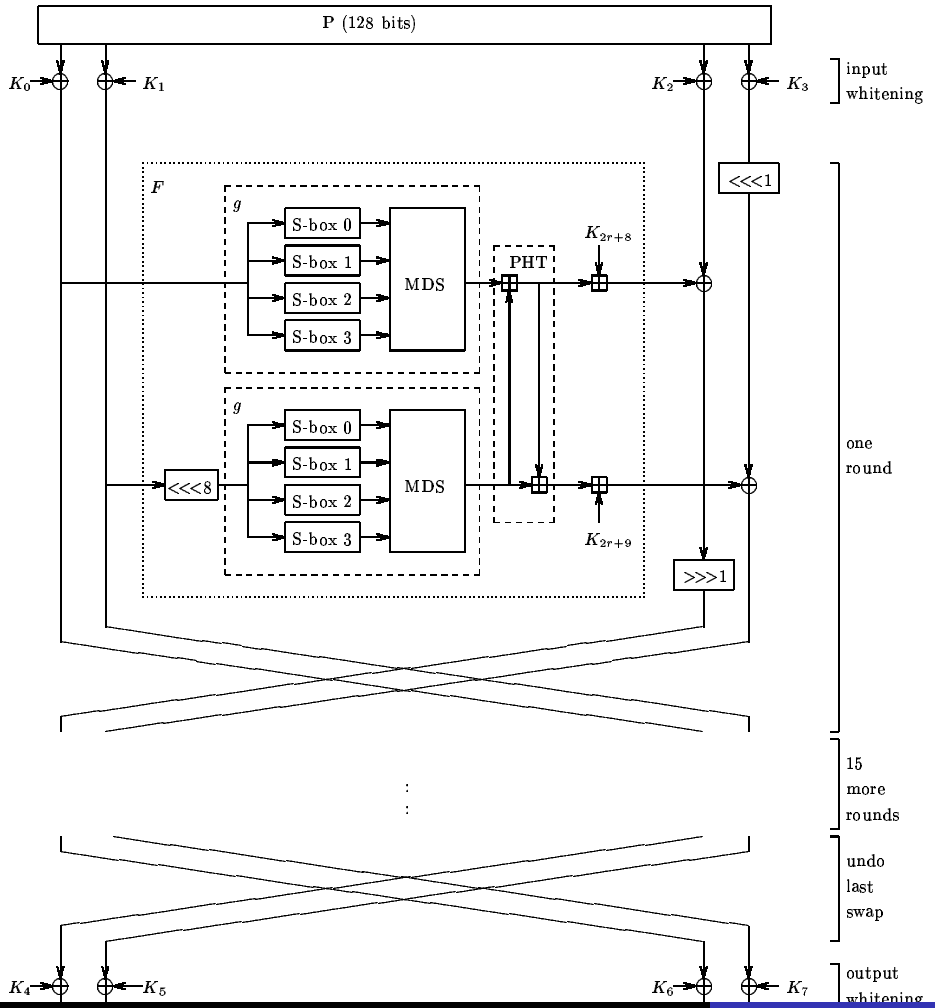
A criptografi a é algo presente em quase todas as civilizações da antiguidade e, ao longo do tempo, foi criando uma vasta tradição de actividade (uma “arte”) mais ou menos obscura.

Está documentado o seu uso nos exércitos de César e de Alexandre; existe evidência do seu uso, ainda antes, nas antigas civilizações maia, indiana e chinesa.

Muitas técnicas criptográfi cas modernas (principalmente as que herdaram as preocupações “clássicas”: cifras simétricas e funções de “hash”) baseiam muita da sua segurança numa mistura de rigor, intuição e experimentação.

Por exemplo, apesar de toda uma teoria de “funções não-lineares perfeitas” (colocada em questão pelo recente desenvolvimento da “criptoanálise algébrica”) o projecto de “S-boxes” é ainda fortemente dependente da experiência e da experimentação.

Um herdeiro da “antiga arte”: a cifra *Two Fish*



Numa perspectiva moderna a função da Criptografi a não se limita à especifi cação e análise de esquemas ou protocolos usando modelos matemáticos mais ou menos rigorosos.

Cada vez mais o seu papel principal resulta de uma observação detalhada do contexto social onde o a tecnologia se insere: que relações são estabelecidas, que direitos devem ser respeitados, que princípios éticos devem ser seguidos, etc.

Esta observação exige experiência e experimentação e tem de ser vista como uma arte.

Tomemos um vulgar par de chaves pública e privada. Não é necessária uma defi nição muito complicada de segurança para concluir:

A **chave privada** é tão mais segura quanto menos conhecida for.

Idealmente a chave privada deve constituir **conhecimento** de um e só um agente: deve ser um **segredo** específi co desse agente.
A capacidade para um agente garantir os seus direitos está associada à sua **identidade criptográfi ca** que, computacionalmente, é indistinguível dos segredos que o agente detém.

Logo

$$\textit{segredos} \implies \textit{direitos}$$

. . . ao invés . . .

A **chave pública** é tão mais segura quanto mais conhecida for.

Quanto mais conhecida mais está ao abrigo de uma **fraude por substituição** (que seria muito fácil de detectar).

Idealmente uma chave pública deve ser universalmente conhecida e, dessa forma, reconhecida como legítima: isto é, quanto mais conhecida mais alargada é a **confi ança** que nela é depositada, individualmente, por cada agente.

Quanto maior é a confi ança maior á a **crença** que do seu uso legítimo não resulta nenhuma **violação de direitos** de cada agente que a reconhece.

Logo

$$\textit{confiança} \implies \textit{direitos}$$

Segredos

Segredos (quer sejam designados por “chaves”, “códigos secretos”, “passwords” ou PINs) sempre estiveram no centro da Criptografi a.

Isto porque a noção de **identidade criptográfica**, traduzida na capacidade de um agente decifrar mensagens, aceder a recursos ou de autenticar actos, é indistinguível dos segredos que detém.

Como consequência, a quase todas as técnicas criptográfi cas acabam por ser expressas na noção geral de **computação na presença de segredos** ou **computação na presença de conhecimento**.

Computações criptográfi cas: noções essenciais

Complexidade e **intratabilidade** computacionais

por experiência (ou ausência dela) certas computações são consideradas computacionalmente intratáveis: a factorização de grandes inteiros, a indexação em certos grupos cíclicos, etc.

a segurança de todas técnicas criptográfi cas parte dessa suposição.

conhecimento e encadeamento

para produzir um resultado uma computação usa o estado de conhecimento que resultou de computações anteriores e gera um novo estado de conhecimento que será usado na computação seguinte.

Os segredos deixam de o ser quando existe uma computação tratável que, a partir de um estado de conhecimento, os gere.

aleatoriedade:

o resultado e o estado do conhecimento dependem, quase sempre, de factores aleatórios e têm de ser calculado num espaço de probabilidade

As técnicas criptográfi cas classifi cam-se pela forma como, computacionalmente, lidam com o conhecimento.

Primitivas: são simples funções matemáticas $f : \{0,1\}^* \rightarrow \{0,1\}^*$ que transformam, sem afectar nem ser afectadas por conhecimento, string de bits em strings de bits.

Esquemas: são computações criptográfi cas que lidam com o conhecimento e com a aleatoriedade. Distinguem-se dos protocolos pelo facto de usarem o conhecimento de um único agente.

Protocolos: Computações ainda mais complexas envolvendo interacções entre dois ou mais agentes. Cada agente dispõe de uma sequência de computações (uma **estratégia**) que usa, com o seu conhecimento próprio, em função de dos “inputs” recebidos de outros agentes.

Exemplo: Componentes de cifras, como S-boxes, matrizes de difusão, etc. são exemplos de primitivas. Também a cifra RSA, na presença da chave, é uma primitiva criptográfi ca.

Já as cifras e as assinaturas digitais não determinísticas são exemplos de esquemas criptográfi cos.

Identifi cação de agentes, acordo de chaves, etc., já são técnicas criptográfi cas que requerem protocolos.

conhecimento e aleatoriedade são duas apresentações do mesmo conceito: o de entropia.

Exemplo: Um atacante tem de adivinhar o valor de 1 bit de segredo.

computando um bit aleatório, se não tiver qualquer conhecimento do segredo, a probabilidade de acertar será $1/2$; é “unbiased”.

consoante aumenta o conhecimento sobre o segredo, a probabilidade de acertar no valor correcto do bit cresce; no limite a probabilidade é 1 quando o segredo for completamente conhecido.

Nota: adivinhar um segredo de n bits é equivalente a adivinhar n vezes um segredo de 1 bit tendo em atenção que, ao adivinhar o bit de ordem k, já são conhecidos os $k - 1$ bits anteriores.

Conhecimento zero

Um atacante tenta adivinhar o valor de 1 bit interagindo com o detentor do segredo através de um determinado protocolo fi nito.

se, qualquer que seja a estratégia (sequência de computações) usada pelo atacante, o resultado é “unbiased” o protocolo diz-se de **conhecimento zero**.

O mecanismo *login/password* não é, obviamente, de conhecimento zero.

Confi ança

Confi ança é uma relação entre um agente e outro agente que resulta da **crença** que o primeiro tem de que qualquer eventual acto do segundo não irá constituir violação de direitos seus.

A confi ança num agente é corporizada na sua **identidade** e transfere-se para os seus actos e para o conhecimento que daí resulta; actos e conhecimento têm um **autor** e a confi ança que neles é depositada é a que é transferida pelo autor.

A confi ança numa identidade, acto ou conhecimento pode ser axiomática (“confi ança cega”) ou resultante de uma **prova** e do **reconhecimento** dessa prova.

Exemplo: Uma **chave pública** é um item de conhecimento em que a confi ança nele depositada depende de uma prova.

Neste caso a prova é o **certificado de chave pública** e o seu “reconhecimento” é um esquema criptográfi co que envolve a verifi cação de uma assinatura digital.

O reconhecimento é um mecanismo para “adiar a confi ança” já que transfere o ónus de depositar confi ança no item inicial para o depositar confi ança no autor da prova.

O autor é a a **autoridade de certificação** que emitiu o certifi cado; a confi ança que nele se deposita ou é cega (caso seja uma autoridade raiz) ou então é fundada noutra prova, que também necessita de reconhecimento, e o processo repete-se.

Exemplo: *Identity Based Criptography* defi ne uma família de técnicas criptográfi cas sugeridas alguns anos (*Shamir, 1984*) mas que só nos últimos anos adquiriu importância.
Essencialmente a ideia base é a seguinte:

1. `Alice` quer enviar uma mensagem a `Ze` com prazo de validade limitada (p.ex. amanhã)
2. `Alice` cifra uma mensagem com a chave pública por si escolhida; p.ex., `Ze-nao-depois-de-8Nov05`
3. `Ze` obtém de uma autoridade (designada PKG - “Private Key Generator”) a chave privada que lhe permitirá decifrar a mensagem se isso estiver dentro do contrato pré-estabelecido entre os três agentes.

O tratamento da confi ança é, aqui, perfeitamente distinta da do exemplo anterior.

Toda a técnica criptográfi ca pode ser expressa neste quadro a duas dimensões: segredos e confi ança.

o tratamento da confi ança é, essencialmente, dual do tratamento dos segredos; nomeadamente

- a noção de **reconhecimento** é dual da noção de **computação**,
- a noção de **identidade** é dual da noção de **conhecimento**,
- genericamente, a noção de **crença** é dual da noção de **cálculo**

. . . porque . . .

reconhecimento/computação
o reconhecimento transfere o ónus da crença ao longo de uma cadeia de outros reconhecimentos; uma computação transfere o ónus do cálculo ao longo de uma cadeia de outras computações,

identidade/conhecimento
uma computação usa conhecimento e produz novo conhecimento e um resultado (dentro de um espaço de probabilidade); o reconhecimento usa uma identidade e produz uma nova identidade e um resultado do reconhecimento.

Divaguei sobre aquilo que me parece ser a essência da moderna criptografi a; nomeadamente sobe

- a difi culdade de identifi car, especifi car e formalizar os seus objectivos afastando-me das visões mais deterministas que têm surgido na literatura; daí a minha classifi cação da disciplina como uma *arte*,
- a importância de defi nir um quadro referencial que dê igual importância ao tratamento do conhecimento (segredos) como da confi ança.

  enquanto que o tratamento do conhecimento está amplamente documentado na literatura o tratamento da confi ança está praticamente ausente.

Espero não ter afastado muita gente da disciplina

Obrigado pela atenção