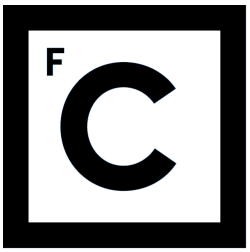
Introdução à Teoria dos Números
Aplicações Criptográficas II



Ciências
ULisboa

Faculdade
de Ciências
da Universidade
de Lisboa

Diogo Sousa · desousa [at] fc.ul.pt

2 de Abril de 2019

Resumo

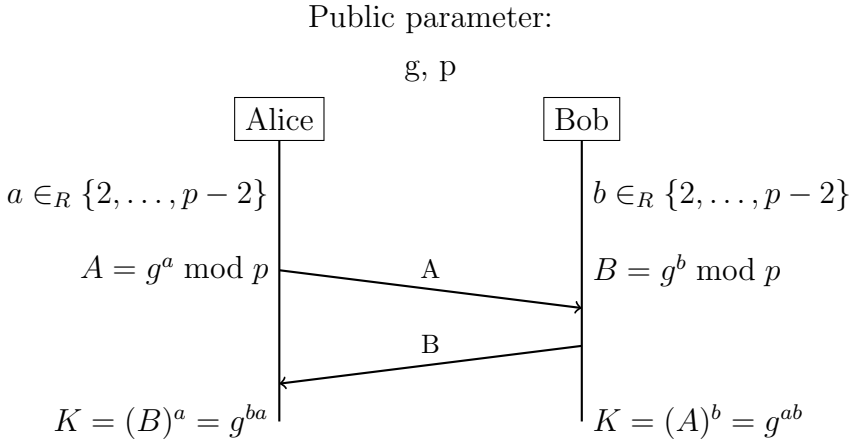
Neste guião iremos abordar dois mecanismos chave da criptografia assimétrica:
- A troca de chaves Diffie–Hellman
- O sistema criptográfico RSA

Vamos comparar a sua robustez teórica com as questões práticas de uma implementação funcional.

Introdução

Como já referido antes, a criptografia é ubíqua na nossa vida moderna. Quando acedemos a um site através do protocolo HTTPS, obtemos garantias sobre a confidencialidade e integridade dos dados que são transmitidos. A comunicação entre cliente e servidor baseia-se na existência de uma **chave de sessão**, nunca utilizada antes, para cifrar as comunicações de forma contínua através de cifra simétrica (AES-GCM geralmente).
Como é que dois interlocutores que não se conhecem e não tiveram tempo para definir um segredo de antemão conseguem comunicar desta forma em segurança? Entra o protocolo de troca de chaves Diffie–Hellman.

Diffie–Hellman



O protocolo é relativamente simples e está amplamente documentado, portanto vou escusar-me de o reproduzir aqui. A sua força assenta na dificuldade[1] de resolver o problema do logaritmo discreto. Vamos focar-nos nos requisitos práticos do sistema.
Segue-se um conjunto de questões cujas respostas ilustram os pontos chave:

1. Porque é que p não pode ser um número composto de igual dimensão? O problema do logaritmo discreto não é igualmente difícil?
2. p pode ser um primo qualquer?
3. Porque é que g tem de ser uma raiz primitiva?
4. Dado p, como é que encontramos rapidamente g?
5. É possível manipular o protocolo para obter um K pré-definido? Requer manipular ambas as partes?

[1] Dificuldade sugerida. O problema não está provado como computacionalmente difícil.

RSA

Este é outro sistema amplamente conhecido. O ponto a ter em consideração é que uma **chave pública** é um tuplo (e, n) em que e é o nosso expoente público, geralmente $2^{16} + 1$, e uma **chave privada** é um tuplo (d, n) onde d é o inverso modular de e em $\bmod n$. Este criptosistema está neste momento a cair em desuso, devido ao problema do tamanho de chaves. Existem novos sistemas, como o ECC, que fornecem segurança equivalente para um tamanho de chaves muito menor.
Aqui vamos abordar os problemas possíveis que enfraquecem o sistema RSA:

1. Reutilização de chaves: porque n tem de ser único? Como garantir isso?

2. Porque utilizamos e como $2^{16}+1$ e não outro valor qualquer? Não podíamos colocar a segurança só do lado da chave privada?

3. Que cuidados devem ser tidos a escolher p e q?

4. Seja m a nossa mensagem e consideremos que é um *byte*. Qual o problema de definir as nossas operações de cifra e decifra da seguinte forma:
   $E(m, K_{pu}) = m^e \bmod n = m'$
   $D(m', K_{pr}) = (m')^d \bmod n = m^{ed} \bmod n = m^{\Phi(n)} \times m \bmod n = 1 \times m \bmod n$

Exercício

Problem 407 - Idempotents

Idempotents

If we calculate a^2 mod 6 for $0 \le a \le 5$ we get: 0,1,4,3,4,1.

The largest value of a such that $a^2 \equiv a \bmod 6$ is 4.
Let's call M(n) the largest value of $a < n$ such that $a^2 \equiv a \pmod{n}$.
So M(6) = 4.

Find $\sum M(n)$ for $1 \le n \le 10^7$.

Para uma versão mais simples, podem calcular os valores para $1 \leq n \leq 10^5$.
Para referência, o resultado para 10^4 é 34981569.