EXAME Fundamentos de Criptografia
CURSO MI/MEI - CSSI

DURAÇÃO 2:00
09·Julho·2013

I

Existe um relação estreita entre códigos lineares e problemas com relevância criptográfica. Nomeadamente são importantes *códigos binários cíclicos* que usam, com estrutura base, determinados anéis de polinómios de coeficientes em $\mathbb{F}_2$;

1. Como se define um código binário cíclico: que anéis de polinómios são usados e como se define codificação e descodificação.
2. O criptosistema de McEliece foi pioneira na introdução de uma abordagem para definir funções "one-way trapdoor". Como é que este criptosistema consegue usar um código linear para definir uma tal função.

II

Os grupos cíclicos, e em particular os grupos Diffie-Hellman, fornecem o suporte formal para muitas técnicas criptográficas;

1. Defina os problemas DLP ("discret log problem"), CDHP ("computation Diffie-Hellman problem") e DDHP ("decision Diffie-Hellman problem") num grupo cíclico aditivo $\langle G, +, 0\rangle$.
2. Com o conhecimento atual, que grupos concretos fundamentam técnicas criptográficas que exploraram o "gap" CDHP-DDHP? Dê um exemplo de uma tal técnica.
3. Num grupo cíclico G a complexidade para resolver o DLP é determinada pelo maior fator primo da sua ordem $|G|$. Porquê?

III

A cifra El Gamal e a assinatura DSA são exemplos de técnicas criptográficas em grupos cíclicos.

1. Porque é que o El Gamal é uma cifra segura contra ataques de texto claro conhecido.
2. Descreva o DSA e indique porque é seguro: um atacante, mesmo que conheça uma sequência de pares (mensagem,assinatura), se não conhecer a chave privada é incapaz de construir uma assinatura para uma mensagem nova.
3. Num grupo cíclico onde o DDHP seja simples e o CDHP seja complexo, é possível implementar um esquema de assinaturas muito menos complexo que o DSA. Como?

IV

Basear uma técnica criptográfica em problemas que, no caso geral, são difíceis apenas "no pior caso", não dá suficiente confiança à sua segurança. É mais seguro basear a técnico num problema que é difícil "no caso médio", ou, ainda melhor, "no melhor caso".

1. Justifique a afirmação anterior ilustrando-a numa técnica, como o RSA, que é baseado na dificuldade em fatorizar inteiros.
2. Resuma o que sabe sobre a segurança do RSA.
3. O "pigeon hole principle" (PHP) permite definir situações onde a complexidade de exprime no "melhor caso". Defina o problema e indique a sua complexidade.