EXAME Criptografia e Segurança da Informação — DURAÇÃO 2:30
CURSO MEI — 3·Setembro·2015

I

Existe um relação estreita entre códigos Reed-Solomon e o designado "problema da reconstrução polinomial com ruído" (NPR).

1. Descreva o problema e discuta as circunstâncias em que é criptograficamente "difícil".
2. Como é que a solução de NPR é usada nos códigos Reed-Solomon?
3. Como é possível transformar o criptosistema de McElice de modo a usar códigos de Reed-Solomon em vez de códigos de Goppa?

II

Curvas elípticas determinam grupos cíclicos criptograficamente relevantes que são uma alternativa aos grupos multiplicativos de inteiros usados na versão original do "Digital Signature Algorithm" (FIPS 186-1, 1994).

1. Descreva de que forma se constroem os grupos cíclicos de uma e de outra forma.
2. Que vantagens e desvantagens existem na utilização de um e outro tipo de grupo cíclico.
3. Os grupos em curvas elípticas permitem, adicionalmente, construir "emparelhamentos". Defina emparelhamentos e dê um exemplo da sua relevância criptográfica.

III

A Criptografia de Chave Pública desenvolveu-se em torno de dois problemas considerados difíceis: a fatorização e o logaritmo discreto em anéis/grupos de inteiros.

(a) Em relação ao problema da fatorização de inteiros:
   1. Como ele intervém na segurança das técnicas RSA? Como ele se relaciona com o problema da ráiz quadrada modular?
   2. Um atacante com acesso a metade dos bits de um fator do módulo RSA, consegue fatorizar completamente esse módulo: como?

(b) Em relação ao problema do logaritmo discreto no grupo multiplicativo $\mathbb{Z}_p^*$, com p primo:
   1. Em que condições a ordem do grupo permite uma solução eficiente deste problema?
   2. Será que uma solução do *problema do número escondido* permitiria resolver o problema do logaritmo discreto a partir de conhecimento parcial (alguns bits) dessa solução?

IV

(a) O teorema de Coppersmith, na sua versão mais simples, usa a técnica das dependências lineares para, dados $f \in \mathbb{Z}[x]$ e N, encontrar "pequenos" inteiros x que verifiquem $f(x) \equiv 0 \bmod N$. Genericamente, o que é a técnica das dependências lineares e como é que ela se relaciona com a redução de bases em reticulados?

(b) Como é que o teorema de CopperSmith usa dependências lineares e mudanças de base para encontrar raízes modulares de polinómios.

(c) Como é que se pode usar o teorema de Coppersmith para resolver o problema da descodificação Reed-Solomon.