EXAME Criptografia e Segurança da Informação — DURAÇÃO 2:30
CURSO MEI — 14·Fevereiro·2015

I

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?

II

(a) A reconstrução polinomial com erro e suas variantes, formam uma família de problemas essenciais em muitas técnicas criptográficas e de codificação da informação.

1. Descreva o problema principal e as variantes mais importantes. Em que circunstâncias o problema é "hard"?
2. Diga como o problema da reconstrução polinomial é fundamental à descodificação de um código Reed-Solomon e porque é que o teorema de Coppersmith, na versão polinomial, determina as condições em que a descodificação é possível?

(b) 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 $f(x) \equiv 0 \bmod N$.

1. Genericamente, o que é a técnica das dependências lineares e como é que ela se relaciona com a redução de bases em reticulados?
2. Como é que o teorema de CopperSmith usa dependências lineares e mudanças de base para encontrar raízes modulares de polinómios.

III

Curvas elípticas sobre $\mathbb{F}_q$, com p primo, são uma componente de muitas técnicas criptográficas.

1. O que é uma curva elíptica sobre $\mathbb{F}_q$ e porque é que tal curva tem interesse criptográfico?
2. Defina estrutura de torsão em curvas elípticas sobre $\mathbb{F}_q$. Qual é a importância da escolha do grupo de torsão nas aplicações criptográficas das curvas elípticas?
3. O que é uma função emparelhamento sobre uma curva elíptica, e porque é que é criptograficamente importante?
4. Descreva a implementação da cifra ElGamal usando um grupo de torsão numa curva elíptica?