EXAME Fundamentos de Criptografia
CURSO MEI- Edição ISTM

DURAÇÃO 2:30
·Julho·2015

I

A Criptografia de Chave Pública desenvolveu-se ao longo dos anos 70's e 80's em torno de dois problemas considerados difíceis: a fatorização e o logaritmo discreto em anéis/grupos de inteiros.

1. Descreva o problema da fatorização de inteiros. Como ele intervém na segurança de técnicas criptográficas da família RSA.
2. Os melhores algoritmos de fatorização têm classe de complexidade sub-exponencial. O que significa esta afirmação? É possível distinguir o "pior caso" do "caso médio"?
3. O problema do logaritmo discreto têm soluções simples se os parâmetros forem mal escolhidos. Em que condições a ordem do grupo multiplicativo $\mathbb{Z}_p^*$ (com p primo) permite uma solução eficiente do problema do logaritmo discreto?
4. Descreva sumariamente o esquema de assinaturas DSA e justifique porque é que a sua segurança é comprometida por uma má escolha do primo p (mesmo que seja muito grande).

II

1. A reconstrução polinomial com erro e suas variantes, formam uma família de problemas essenciais em muitas técnicas criptográficas e da codificação da informação. Descreva este problema e diga como é relevante à descodificação de um código Reed-Solomon.
2. Dê uma descrição sumária de esquemas de cifras baseados no problema da descodificação de códigos de Goppa (e.g. McEliece).
3. Polinómios são também usados na cifra NTRU; dê uma descrição sumária desta cifra.
4. Por comparação com cifras assimétricas baseadas na fatorização (RSA) ou no logaritmo discreto (ElGamal), as cifras polinomiais (Mc Eliece e NTRU) têm grandes ganhos em termos de tempos de computação. Justifique esta afirmação e diga qual é a desvantagem básica destes sistemas que limita a sua utilização em dispositivos com pouco poder computacional.

III

Corpos $\mathbb{F}_q$, com um primo q, são essenciais à realização de técnicas criptográficas. Um esquema de assinaturas DSA pode ser realizado diretamente no grupo cíclico $\mathbb{F}_q^*$ ou num grupo de torsão numa curva elípticas sobre $\mathbb{F}_q$.

1. O que é uma curva elíptica sobre o corpo $\mathbb{F}_q$ e porque é que tal curva tem interesse criptográfico?
2. Num tal curva elíptica, o que é um grupo torsão e porque é que tais grupos têm importância crucial no esquema de assinaturas ECDSA.
3. Comparando a realização do esquema DSA em $\mathbb{F}_q$ com similar realização em curvas elípticas (ECDSA), que vantagens relativas tem cada uma destas realizações.
4. O que é uma função emparelhamento sobre uma curva elíptica, e porque é que é criptograficamente importante?