Trabalho prático - I
MO422 – Algoritmos Criptográficos
Prof. Ricardo Dahab[1]

1 Introdução

O trabalho trata da combinação do criptossistema Rabin com ElGamal, para torná-lo probabilístico, atingindo então proteção contra ataques de texto claro escolhido. Em particular, deve ser implementada a versão convencional do criptossistema Rabin, utilizando o Teorema Chinês do Resto para decifração. O tamanho dos parâmetros (módulo N) deve ser fixado em 3072 *bits* de magnitude, para que o nível de segurança atinja pelo menos 128 *bits*. Podem considerar que os primos p e q são sempre tais que $p \equiv q \equiv 3 \bmod 4$.

2 Material

O criptossistema Rabin foi visto em sala e tem segurança equivalente à fatoração de inteiros. Entretanto, uma de suas limitações é sua natureza determinística, o que o torna inseguro contra ataques de texto claro escolhido, quando o espaço de mensagens é muito pequeno. Ao invés de utilizar preenchimento pseudo-aleatório, este trabalho irá explorar como alternativa uma possível combinação com o criptossistema ElGamal para torná-lo mais seguro contra esse tipo de ataque.

Seja um grupo $\mathbb{G}$ com gerador g, instanciado por exemplo a partir de $\mathbb{Z}_r$, com r primo. A chave privada de Alice é um inteiro x selecionado aleatoriamente em $\{1, \ldots, r-2\}$ e a chave pública é $h = (g^x \bmod r) \in \mathbb{G}$. A cifração de uma mensagem m é dada por $c = (c_1, c_2) = (g^y \bmod r, m \cdot h^y \bmod r)$, para um inteiro y escolhido aleatoriamente de $\{1, \ldots, r-2\}$, conhecido como chave efêmera. Observe que o componente c_1 do criptograma é utilizado para transmitir informação sobre a chave efêmera y, enquanto o componente c_2 "mistura" a mensagem m com um elemento aleatório do grupo $\mathbb{G}$ pela multiplicação.

O material para confecção do trabalho prático é de inteira escolha e responsabilidade do aluno. Serão aceitos trabalhos implementados em qualquer linguagem de programação de alto nível ou ambiente de computação algébrica. Sugestões imediatas são Java, por possuir em sua biblioteca padrão suporte a aritmética de precisão arbitrária;

[1]Este trabalho é contribuição do Prof. Diego Aranha

Python, por suportar nativamente inteiros de precisão arbitrária; ou a combinação da linguagem C com a biblioteca GMP (`http://gmplib.org`). Outras alternativas são MAGMA, Maple e Matlab.

3 Objetivo

O objetivo do trabalho é implementar suporte tanto à cifração quanto à decifração da combinação entre Rabin e ElGamal, de forma que o criptossistema resultante seja consistente. Ou seja, a decifração deve entregar exatamente o texto claro processado pelo algoritmo de cifração.

4 Avaliação

É imprescindível a entrega de código funcional e um breve relatório descrevendo a experiência. O documento deve também tratar das seguintes questões:

- Qual o impacto em desempenho de sua proposta, comparado ao Rabin tradicional?
- Há ambigüidade no processo de decifração? Como é possível eliminá-la?
- Por que o criptossistema resultante se tornou resistente contra ataques de texto claro escolhido?
- Quais as premissas de segurança (dificuldade de problemas) em que está baseada a segurança do criptossistema proposto? Como se compara com o Rabin tradicional?

O prazo de entrega é **24 de outubro** e o trabalho é individual. **A qualidade da sua implementação será levada em consideração, além da corretude.**