

Universidade do Minho

Lic. em Matemática e Ciências de Computação

Criptografia Aplicada

2007/2008

Construção das Tabelas Características das *S-Boxes* do DES

Rui Carlos A. Gonçalves (41031)

4 de Dezembro de 2007

Resumo

Neste relatório descreve-se de forma sucinta o trabalho realizado no âmbito da disciplina de Criptografia Aplicada, onde se pretendia desenvolver uma aplicação que construísse as tabelas características das *S-Boxes* do DES.

1 Introdução

Desenvolvida no início da década de 90 do século passado, a criptoanálise diferencial é uma técnica que pode ser usada para atacar o DES, e que explora as relação entre as diferenças entre os *bits* à entrada e à saída das várias *S-Boxes*. O facto destas diferenças não serem tão aleatórias quanto desejável, possibilita que se determinem valores para a chave mais prováveis do que outros.

A primeira fase deste ataque consiste em obter as tabelas que, para cada uma das *S-Boxes*, registam para cada diferença possível entre um par de *inputs*, as diferenças entre os pares de *output*. O objectivo deste trabalho é precisamente a construção dessas tabelas. Adicionalmente, pretende-se também saber quais os pares que verificam uma diferença no *input* e no *output* dadas.

2 Implementação

Para atingir os objectivos propostos, foram criadas duas classes Java (a linguagem escolhida para a implementação do trabalho), uma que representa as várias *S-Boxes* do DES (a classe `SBox`), e outra que calcula as tabelas e determinam o conjunto de pares que verificam determinadas diferenças (a classe `Diff`).

Assim, a classe `SBox` armazena as várias tabelas correspondentes às *S-Boxes*, e disponibiliza um método (`byte get(byte in, int sbox)`), que para um conjunto de 6 *bits*, e uma determinada *S-Box*, devolve o respectivo conjunto de 4 *bits* resultante da transformação do *input*.

A classe `Diff`, implementa 3 métodos, que se descrevem de seguida:

- `int[] line(byte diff_in,int sbox)`
Para uma determinada diferença na entrada, e para uma *S-Box*, devolve a contagem do número de ocorrências de cada uma das 16 diferenças possíveis à saída;
- `int[] [] table(int sbox)`
Constrói a tabela característica de uma *S-Box*, isto é, para cada uma das diferenças possíveis à entrada, devolve a contagem do número de ocorrência de cada diferença à saída;
- `ArrayList<byte[]> pairs(byte diff_in, byte diff_out, int sbox)`
Dada uma diferença de entrada e uma diferença de saída, devolve o conjunto de pares que as varificam.

Para além da API disponibilizada pelas classes anteriores, temos ainda a classe `Main` que nos permite usar directamente as funções. Assim, a função `main`, para a opção `-t <S-Box>`, imprime a tabela característica correspondente à *S-Box* dada, e para a opção `-p <diff_input> <diff_output> <S-Box>`, imprime os pares que têm uma determinada diferença à entrada e uma determinada diferença à saída, para um *S-Box* específica.

3 Conclusão

Não havendo grandes questões em torno da sua implementação, a realização deste trabalho permitiu sobretudo perceber melhor como *funciona* este tipo de criptoanálise, e como esta pode ser usada para atacar uma cifra por blocos, em particular o DES.

Referências

- [1] J. B. Almeida. *Apontamentos de Criptografia Aplicada*. Universidade do Minho, 2007.
- [2] *DATA ENCRYPTION STANDARD (DES)*. U.S. DEPARTMENT OF COMMERCE / National Institute of Standards and Technology, 1999.
- [3] <http://wikipedia.org>