Differential Cryptanalysis of Block Ciphers

Matthew Laten

Third Year Maths Project

Supervisor: Dr Christine Swart

“Two can keep a secret if one is dead...” - Anon

Abstract

We begin by discussing basic Probability Theory, along with Block Ciphers and Differential Properties of S-Boxes. We then move on to explaining how a Differential Attack works, and the properties of involved that make it work. Furthermore, we include and implemented case of a Block Cipher break.

Contents

Chapter 1

Introduction

Imagine a world without encryption. Anyone with access to a computer could steal your money, impersonate you, or learn your secrets. Privacy would be dead. The inability to secure information might even lead to police states, where governments will have to resort to desparate measures to protect their secrets. Fortunately, we do not live in such a world. We live in a world where encryption is a very real part of our daily lives. Whether banking online, shopping for new items or chatting to your friends on your favourite social network, you are indirectly using various forms of encryption to keep your messages safe, and indicate to computer servers that you are who you say you are.

So if our data is all secure and encrypted, why should we worry more about the subject of Cryptography? In short, our data isn't secure. The premier algorithm for encrypting electronic data from 1979 onwards, known as the Data Encryption Standard (DES), was broken in 1997. Today's encryption standards are tomorrow's broken algorithms. Attackers are constantly looking for better ways to break encrypted data. So we, as cryptographers, have the responsibility to make encryption more secure. How can we do this? By doning a black hat and thinking like an attacker. In this paper, we will be looking at an attack on block ciphers, specifically known as differential cryptanalysis. But first, we should probably define some unfamiliar terminology.

1.1 Terminology

Remark: Note, this paper assumes that you have an adequate knowledge of 3rd year university level Mathematics, but a knowledge of Cryptography or Probability theory is not required, as all concepts necessary for understanding this paper will be explained.

As you might already know, **Cryptography** is the discipline concerned with keeping data secret, or more formally, it is the study and practice of techniques and algorithms for securing the transference of data in the presence of third parties, known as attackers or adversaries. **Cryptanalysis** however, deals with the breaking of these techniques and retrieval of the secret data.

In cryptography, **encryption** refers to the process of converting plaintext, or data that is easily understandable, into ciphertext, that is unintelligible data. The reverse process of converting the cipher text back into plaintext is known as **decryption**. In most cases, this encryption or decryption occurs with the aid of a **key**, a parameter that determines the functional output of the cryptographic algorithm.

Furthermore, there are two main types which come up when discussing key-based cryptography, namely Symmetric-key, and Asymmetric-key or Public-key cryptography. In the case of **Symmetric-key**, the same key is used for encryption and decryption, while with **Asymmetric-key**, a key is made available to the public for encryption, and only those posessing the secret or private key will be able to decrypt messages encrypted with the matching public key.

A **block cipher** is a type of Symmetric-key encryption cipher that operates on a fixed-length "block" of data. This is in contrast to a **stream cipher**, which operates on a potentially infinite stream of data. For the purposes of this paper, we will define a block cipher in more depth later, but at the moment we have enough of a vocabulary to delve into a bit of supporting knowledge.

Chapter 2

Background

Most mathematical concepts require a bit of supporting or background knowledge, and Cryptography is no different. We will start by looking at some basic Probability Theory, and then move on to Block Ciphers and interesting properties surrounding them. Since the amount of Boolean Algebra required to understand this paper is minimal, a short comment on this topic will be included in the Block Ciphers section.

2.1 Probability Theory

By 3rd year level however, a student will not have covered enough Probability Theory to understand what the premise behind a differential attack is; which means that Probability Theory will be discussed in this section. Topics include what it means for and event to have a probability of occuring, how we calculate an event's probability of occuring, and how likely an event is, or string of random events are to occur.

2.2 Block Ciphers

We will be considering Attacks on Block Ciphers later, and thus it makes sense to introduce Block Ciphers as part of the background. In short, Block Ciphers will be defined as algorithms that operate on a fixed amount of bits, using some sort

of symmetric key. They will further be explained and examples will be given.

2.2.1 Vectorial Boolean Functions (S-boxes)

A large part of understanding Block Ciphers, and how to attack them, will be tied up in understanding S-boxes, (which are types of Vectorial Boolean Functions). This section will deal with introducing and explaining them, along with a few examples.

2.3 Differential Properties of S-boxes

Next will be discussed the various differential properties of S-boxes which allow cryptanalysts to mount an attack against a block cipher. These include the property that XORs do not affect differentials, as well as ways to find relationships between input differentials and output differentials of an S-box.

2.3.1 Probabilities of Differential Trails

The previous properties discussed can be combined to give us insight into the probabilites of differentials trails, or in plain English: Given an input differential, how likely or probable is it that a certain output differential occurs. This section will discuss the theory behind probabilites of differentials, as well as practical examples of cases where probabilities do not conform to the norm.

Chapter 3

Differential Attacks

In this chapter, I will discuss the process whereby a differential attack can be mounted against a block cipher. Perhaps the easiest way to do this would be by means of working through the process in various subsections, and then putting it all together in the form of a theoretical discussion of why it works.

Thus, the following subheadings might be useful:

3.1 Choosing Plaintext/Ciphertext Pairs

3.2 Computing Differentials

3.3 Statistical Analysis on Differentials

3.4 Breaking Each Round Key

3.5 Combining it all together

3.6 The Theory Behind It or Why It Works

Chapter 4

Toy Example

In this section, I will expand upon a given toy example and discuss an implementation of a differential cryptanalysis attack on it. Furthermore, I will implement the attack and hope to break the block cipher.

Chapter 5

Conclusion

In the conclusion, I will wrap up what has been discussed in my paper, and mention what can be improved upon in the future.

Bibliography

[1] Eli Biham and Adi Shamir "Differential cryptanalysis of DES-like cryptosystems". *Journal of Cryptogoly*, 4(?):3-72, 1991

[2] Howard M. Heys. "A Tutorial on Linear and Differential Cryptanalysis". *?*, ?(?):?, 19??

[3] . "Differential Cryptanalysis Tutorial". *?*, ?(?):?, 19??