

Differentielle Kryptoanalyse

ARTIKEL KRYPTOGRAPHIE

Windisch, 16. Mai 2020



thirah__vorhangeschloss-schlüssel-computer-icons__nodate

Autoren	Gabriel Nussbaumer und Fabian von Büren
Dozent	Dr. M. Hufschmid
Modul	Kryptographie (kryg)
Hochschule	Hochschule für Technik - FHNW
Studiengang	Elektro- und Informationstechnik

Inhaltsverzeichnis

1	Einleitung	1
2	Historisches	1
3	Funktionsweise	1
4	Sicherheit	1
5	Schluss	1

1 Einleitung

Der Data Encryption Standard (DES) war in den 70 Jahren das damals meist verwendete Verschlüsselungssystem für die zivile Bevölkerung. Mit dem DES konnte in dieser Zeit ein grosser Widerstand gegen Angriffe bewiesen werden. Jedoch mit der Differenziellen Kryptoanalyse, welche im Juli 1990 von Eli Biham und Adi Shamir veröffentlicht wurde, konnten bei Varianten von DES, mit bis 15 Runden, der geheime Schlüssel herausgefunden werden.

Kryptosysteme sind Funktionen, welche darauf basieren mehrere Runden zu durchlaufen. Bei einer Runde von DES sind verschiedene Funktionen enthalten es gibt eine Bit-Permutation, arithmetische Operationen, EXOR-verknüpfungen und die S-Boxen. Die S-Boxen sind nichtlineare Übersetzungstabellen. Der gesamte Verschlüsselungsalgorithmus, die Permutations Tabellen wie auch die Übersetzungstabellen der S-boxen sind öffentlich bekannt. Die Geheimhaltung der Daten hängt also vom zufällig gewählten geheimen Schlüssel ab.

Wird ein Klartextangriff durchgeführt kann die Komplexität der DES Verschlüsselung um die Hälfte reduziert werden, da die Symmetrie durch Komplementierung genutzt werden kann.

$$T = DES(P, K)$$

$$\bar{T} = DES(\bar{P}, \bar{K})$$

Somit entspricht der Wert X dem Bitweise komplementierten Wert \bar{X} . Die Eigenschaft wird bei der Kryptanalyse ausgenutzt indem zwei Klartext-Textpaare P_1, T_1 und P_2, T_2 zur Verfügung stehen und es gilt P_1, \bar{T}_2 oder P_2, \bar{T}_1 . Der Angreifer verschlüsselt P_1 unter allen 2^{55} Schlüsseln K , deren niederwertigstes Bit Null ist. Wenn im Geheimtext der Wert T gleich dem Wert T_1 ist, dann ist der entsprechende Schlüssel K wahrscheinlich der echte Schlüssel. Ist T gleich dem Wert \bar{T}_2 dann ist der Schlüssel wahrscheinlich \bar{K} .

2 Historisches

3 Funktionsweise

4 Sicherheit

5 Schluss