MysteryTwister C3

THE CRYPTO CHALLENGE CONTEST

Recycelte One-Time-Pad

Autor: George Ho

November 2012

Einleitung

Die One-Time-Pad-Verschlüsselung (OTP) kann man auch als Vigenère-Chiffre beschreiben, bei der eine zufällige und lange Buchstabenfolge als Schlüssel verwendet wird. Die Stärke des OTPs basiert auf der Tatsache, dass der Schlüssel vollkommen zufällig ist und deswegen keine Wiederholungen aufweist, die durch Algorithmen wie dem Kasiski- oder Friedman-Test ausgenutzt werden könnten.
Obwohl das OTP perfekte Sicherheit bietet, hat es den Nachteil, dass der zufällige Schlüssel nur einmal verwendet werden darf und genauso lang sein muss, wie die Nachricht selbst. Ansonsten ist die perfekte Sicherheit nicht länger gewährleistet.

Challenge

In dieser Challenge sind drei Nachrichten zu entschlüsseln, die alle mit einem OTP mit **demselben** zufälligen Schlüssel verschlüsselt worden sind. Es handelt sich um Nachrichten in englischer Sprache einer militärischen Kommunikation während eines Krieges.

Gib als Lösung bitte den Namen des Dorfes/der Stadt aus einem der Chiffretexte in Großbuchstaben an. Wenn die Lösung z.B. Massachusetts wäre, gib bitte MASSACHUSETTS ein.

Hinweis: Wenn du einen Teil des Klartextes raten kannst, kannst du den entsprechenden Teil des Schlüssels bestimmen.

Chiffretexte

PERLSTXZDBFONKKYTQPQJFDEKKJODP

QHNNFIJNWSSOTGUJRNOPLMHRESMHVP

OERZTOHXANSASLKWELZBAOJNKSOUOV

Quellenangabe

Diese Challenge basiert auf einer Unterrichtspräsentation im Kurs "Cryptology" am Center for Talented Youth der Hong Kong University of Science and Technology im Sommer 2012.