

HACKERS.MU

UOM CODE WARS

**FIVE HOURS OF CODE.
HACK TILL YOU DROP.**

Open to all University students: The first edition of UoM Code Wars!
Be trained by Hackers.mu members and contribute to real life open-source projects.

Venue: ETB LAB, Engineering Tower, UoM
Date: 21 September 2017

POWERED BY:



telecom
mauritius

PC4

Stream Cipher and Its Variants

Key

Diagram: A block diagram of a stream cipher structure. It shows a sequence of blocks labeled $0, 1, 2, \dots, n-1, n, n+1, \dots, n-1, n$. The first block is labeled 0 . The second block is labeled 1 . The third block is labeled 2 . The fourth block is labeled $n-1$. The fifth block is labeled n . The sixth block is labeled $n+1$. The seventh block is labeled $n-1$. The eighth block is labeled n . The diagram shows a sequence of blocks connected by arrows. The first block is labeled 0 . The second block is labeled 1 . The third block is labeled 2 . The fourth block is labeled $n-1$. The fifth block is labeled n . The sixth block is labeled $n+1$. The seventh block is labeled $n-1$. The eighth block is labeled n . The diagram shows a sequence of blocks connected by arrows. The first block is labeled 0 . The second block is labeled 1 . The third block is labeled 2 . The fourth block is labeled $n-1$. The fifth block is labeled n . The sixth block is labeled $n+1$. The seventh block is labeled $n-1$. The eighth block is labeled n .

CRC Press

Cryptography and Network Security

- **Secure the package:**

`https://github.com/hackersdotmu/Lynx`

RC4

- **RFC:**

RFC 7465



SCENARIO

- RC4 has been declared insecure.
- You have been tasked by hackers.mu to audit every piece of software.
- Find and patch the vulnerabilities.