Randomized Ciphers

Security in Pure Process Abstraction

By Michael Kangethe and Chrispus Kamau

AfricaHackOn 2016

who_are_we

- Michael Kangethe
  Infosec Enthusiast and Researcher

  - Bsc IT, Msc Computer Science
  - Interests:
    - Artificial Intelligence
    - Secure Data Communications
    - Dynamic Cryptosystems

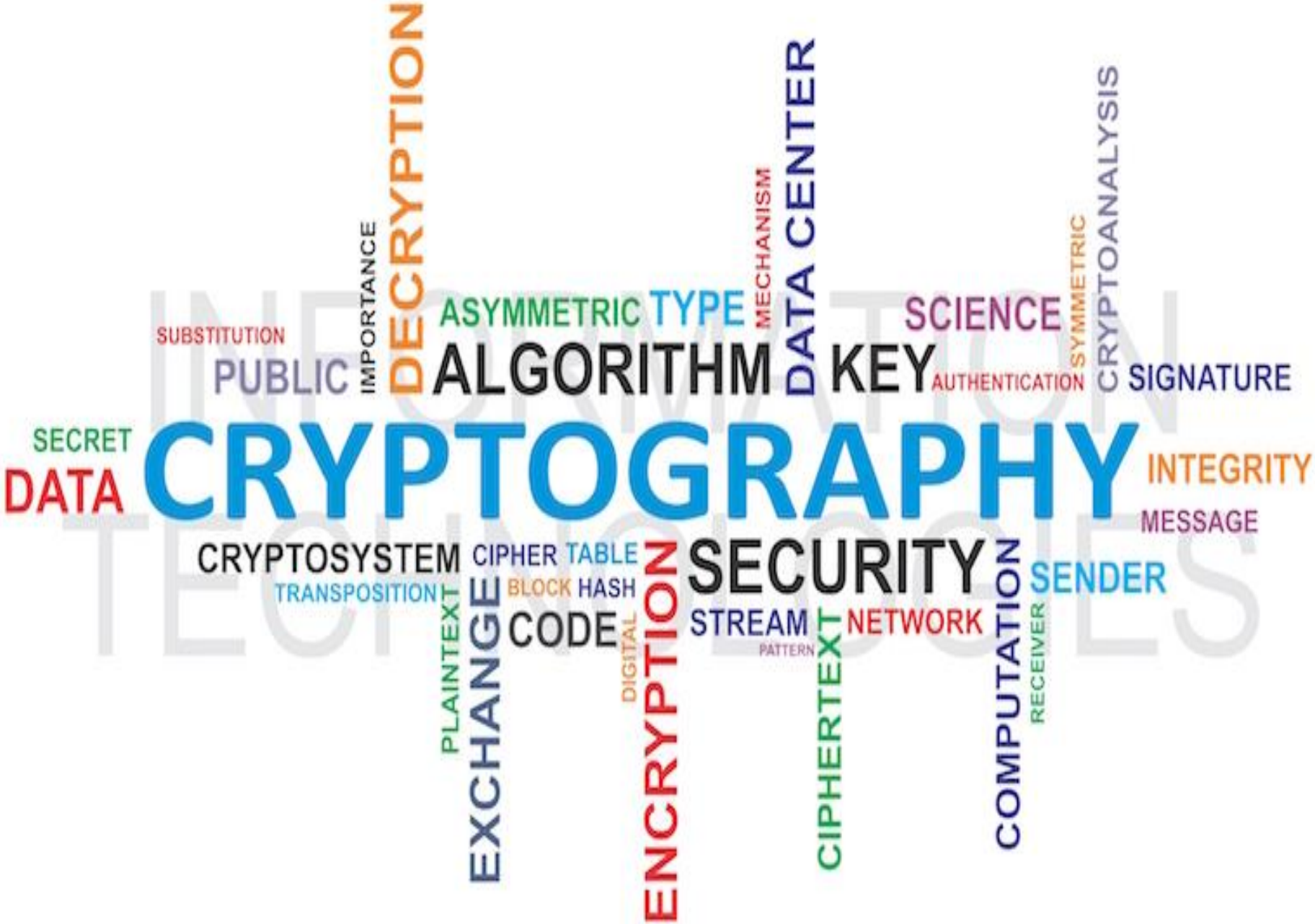
who_are_we

- Chrispus Kamau
  Information Security Engineer

  - Bsc Electrical and Electronics
  - Interests:
    - Radio Frequency
    - Electronics/hardware
    - Mobile device security

What is Encryption

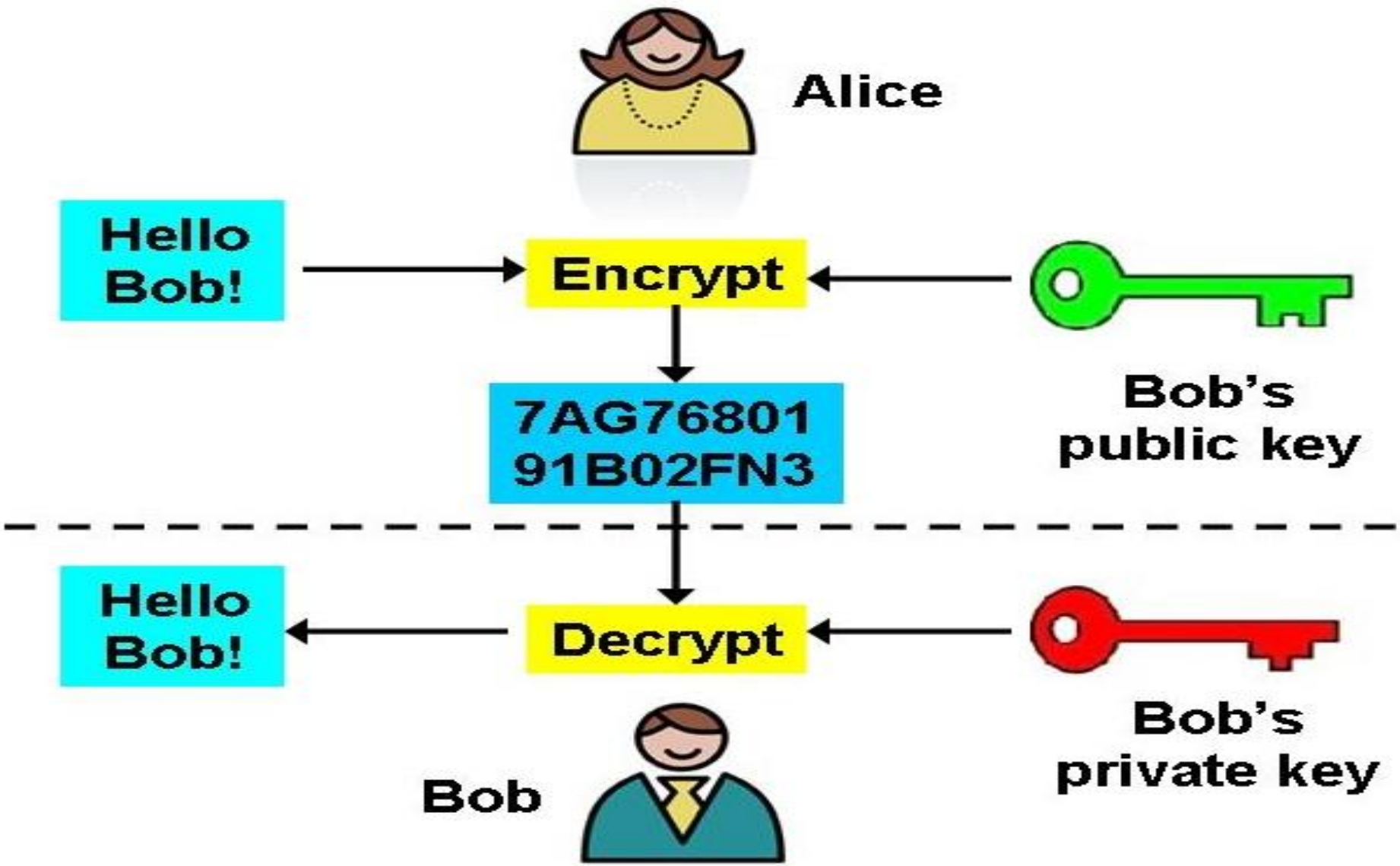
- Encryption is the process of transforming information in such a way that an unauthorized third party cannot read it; a trusted person can decrypt data and access it in its original form though.


CRYPTOGRAPHY
DECRYPTION
DATA CENTER
CRYPTOANALYSIS
ASYMMETRIC
TYPE
MECHANISM
SCIENCE
SYMMETRIC
IMPORTANCE
SUBSTITUTION
PUBLIC
ALGORITHM
KEY
AUTHENTICATION
SIGNATURE
SECRET
DATA
INTEGRITY
MESSAGE
CRYPTOSYSTEM
CIPHER
TABLE
SECURITY
SENDER
TRANSPOSITION
BLOCK
HASH
PLAINTEXT
EXCHANGE
CODE
DIGITAL
ENCRYPTION
STREAM
PATTERN
CIPHERTEXT
NETWORK
COMPUTATION
RECEIVER

Why Cryptography

- Confidentiality
  - Eyes Only
  - Hide your Stash
  - Secure communication e.t.c
- Integrity
  - Data integrity verification
- You MIGHT get HACKED!! So relax and Encrypt

Current Implementations

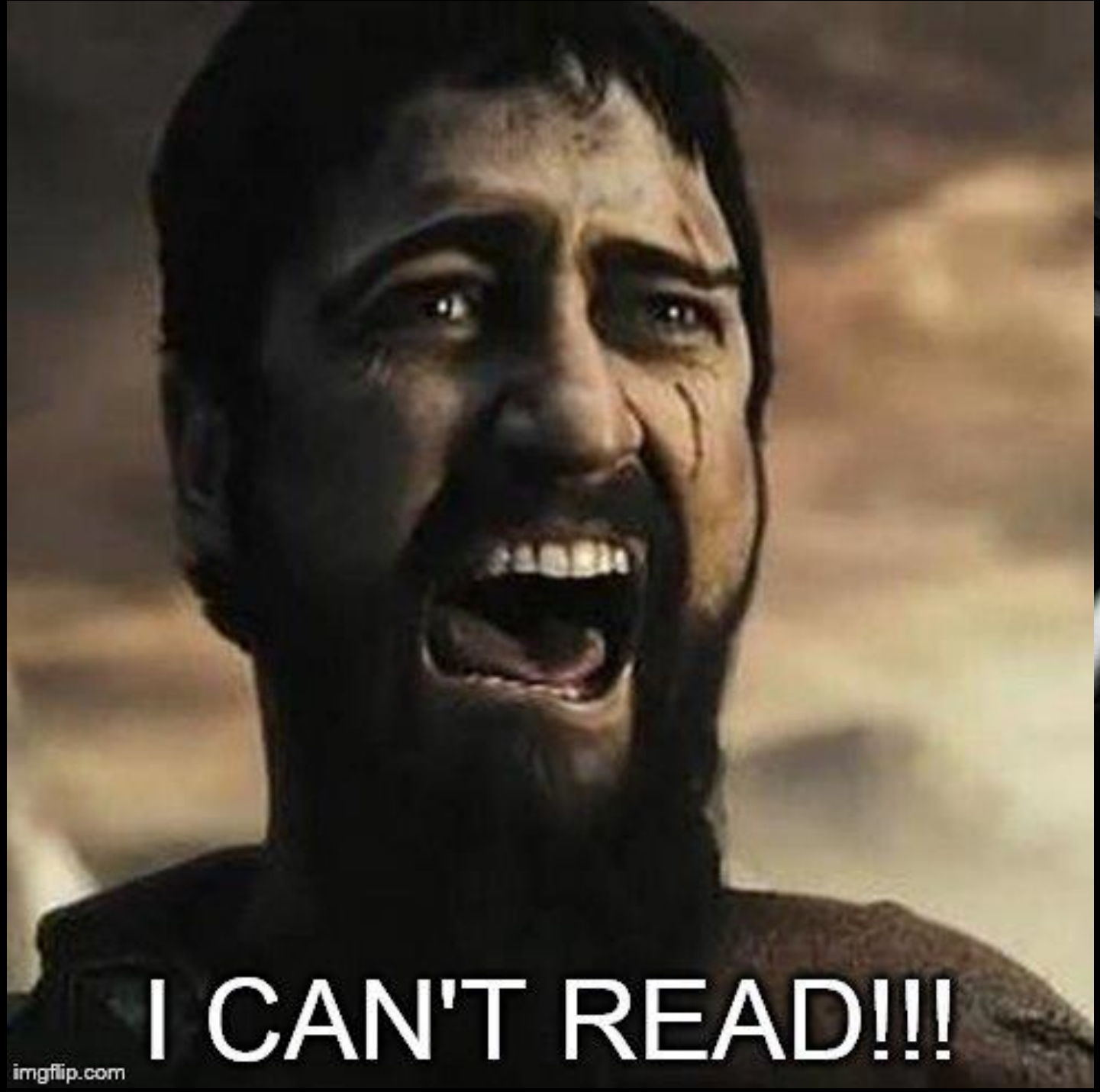


Current Applications

- Confidential Communication
- Secure data storage
  - Files
  - DB Records

Dear Tim,....please find our revenues and profit statement for the last business year attached. This is confidential information.....Best regards..	0stkgNGafvEYc3Vw1JDkv4PVJ+Lk1HFhSmZgQ2hcjtFF1ZvkoFu+y3fAUd4LN/q6TrR8YSnL81Fidsi16CrN7nMAgB36mBVL2gL4hYYGhC+z06K+6PJ1WEZXtMONYqZj3PE1whz8UIZCUsCpnEB

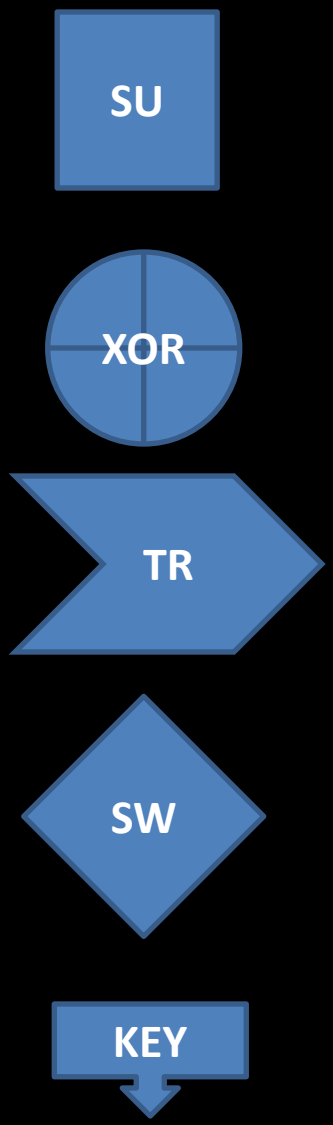
Preferred Reaction


I CAN'T READ!!!
imgflip.com

What Makes a "Secure" Encryption Algorithm?

- The amount of secrecy needed should determine the amount of labor appropriate for the encryption and decryption.
- The set of keys and the enciphering algorithm should be free from complexity.
- The implementation of the process should be as simple as possible.
- Errors in ciphering should not propagate and cause corruption of further information in the message.
- The size of the enciphered text should be no larger than the text of the original message.

What are Ciphers Made of?



Substitution

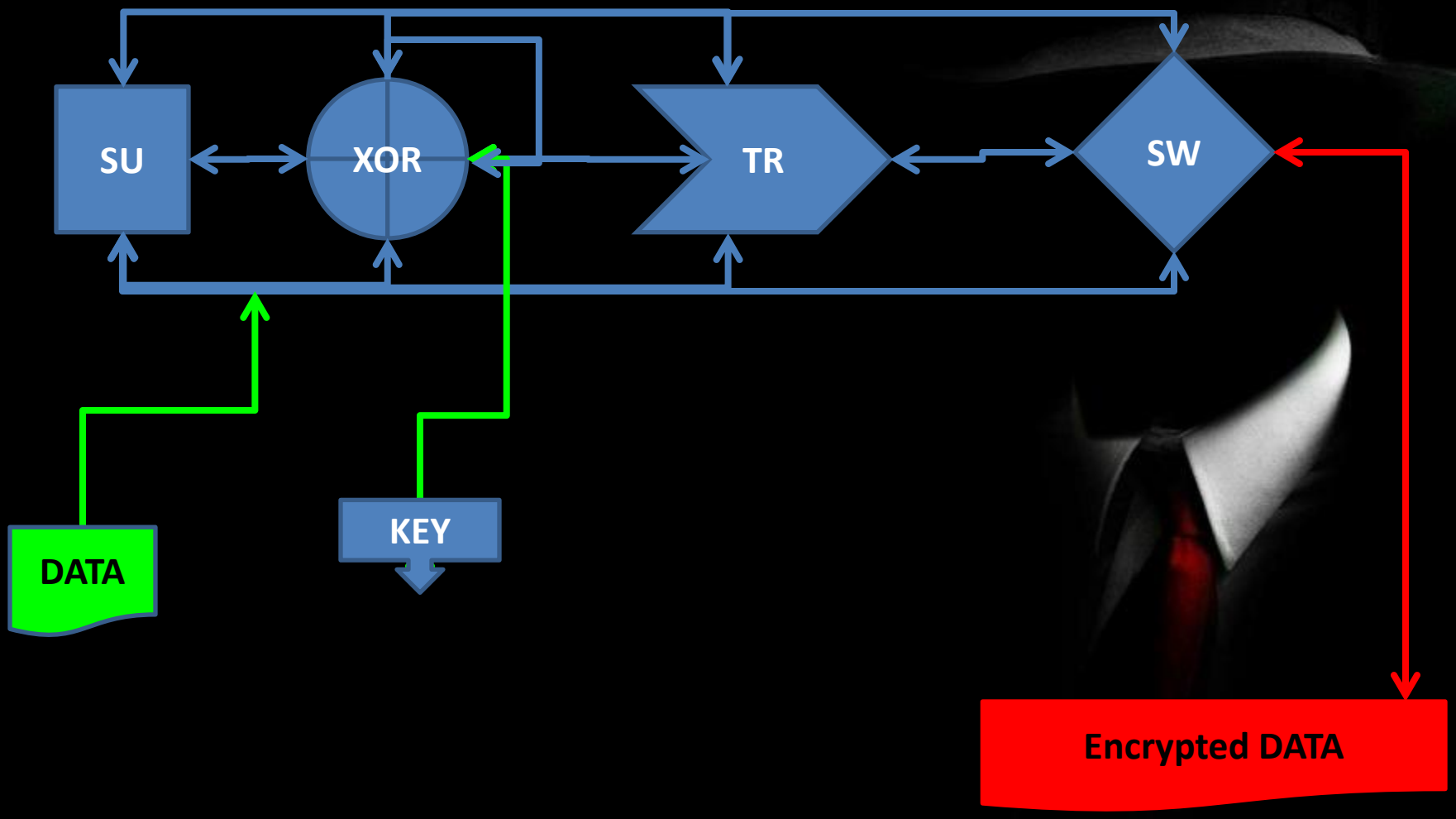
XOR

Transposition

Switching bits

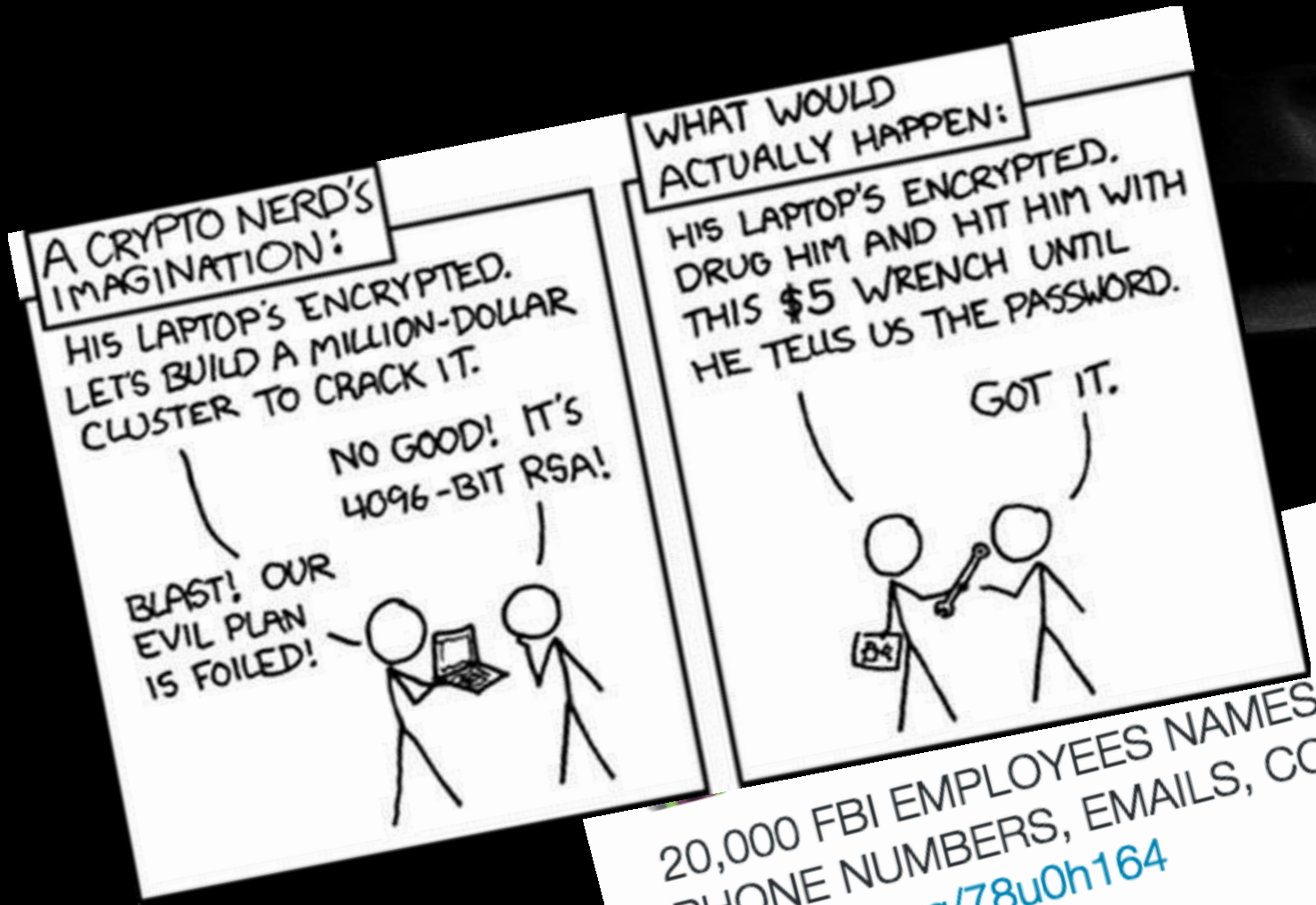
Your Key

Current Ciphers



Problems with Current Ciphers

- Static:
  - Process is known and the same for each Run
  - Once Weakness is found(Broken) Cipher and all implemented Cryptosystems become useless
  - Once process is known one needs to find the Key,
  - Security is based on:
    - Key Size
    - Complexity of Process



Following

20,000 FBI EMPLOYEES NAMES, TITLES, PHONE NUMBERS, EMAILS, COUNTRY
cryptobin.org/78u0h164
password is lol
#FreePalestine

RETWEET
1

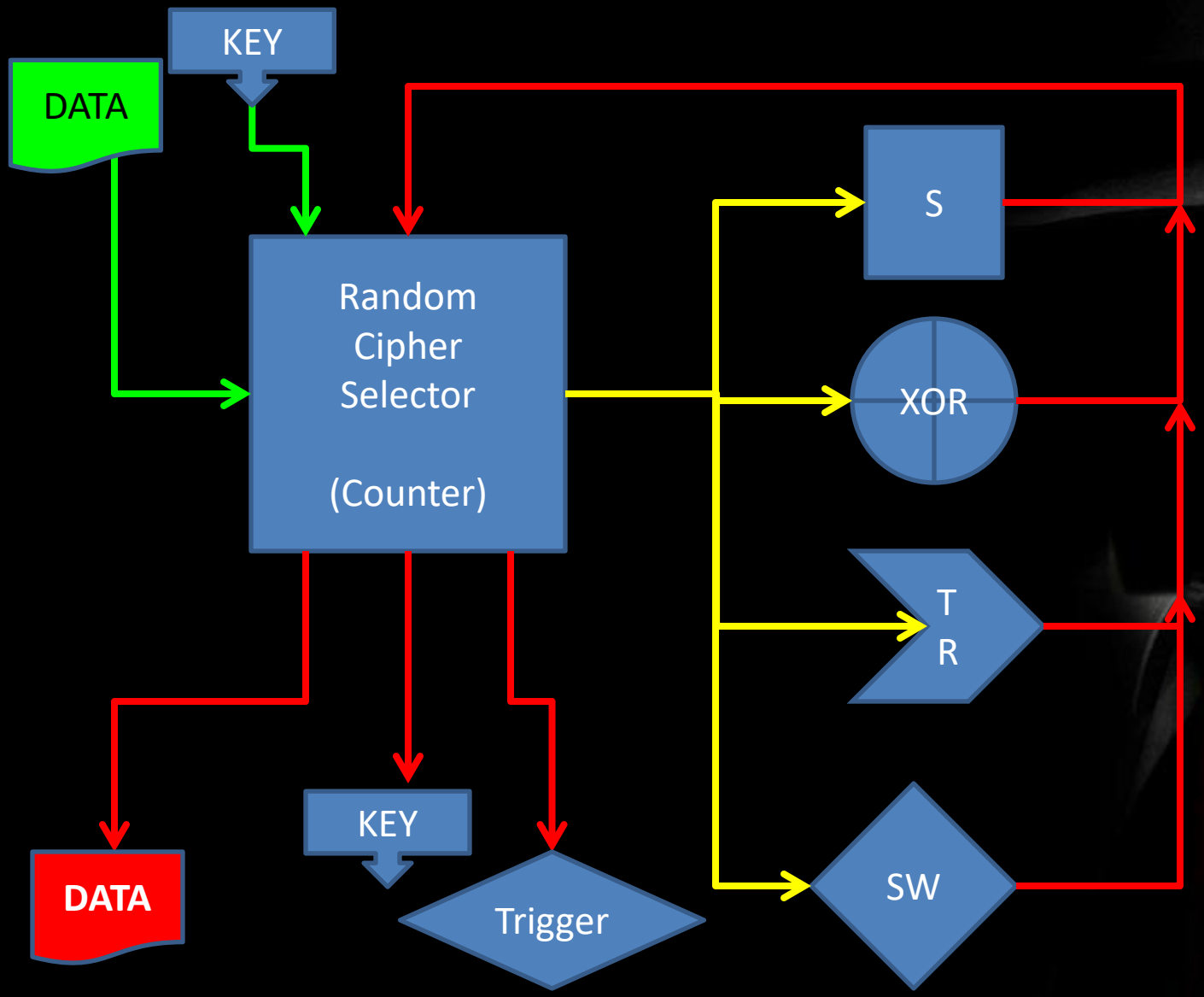
PM - 8 Feb 2016

Facts (Current Cryptosystems)

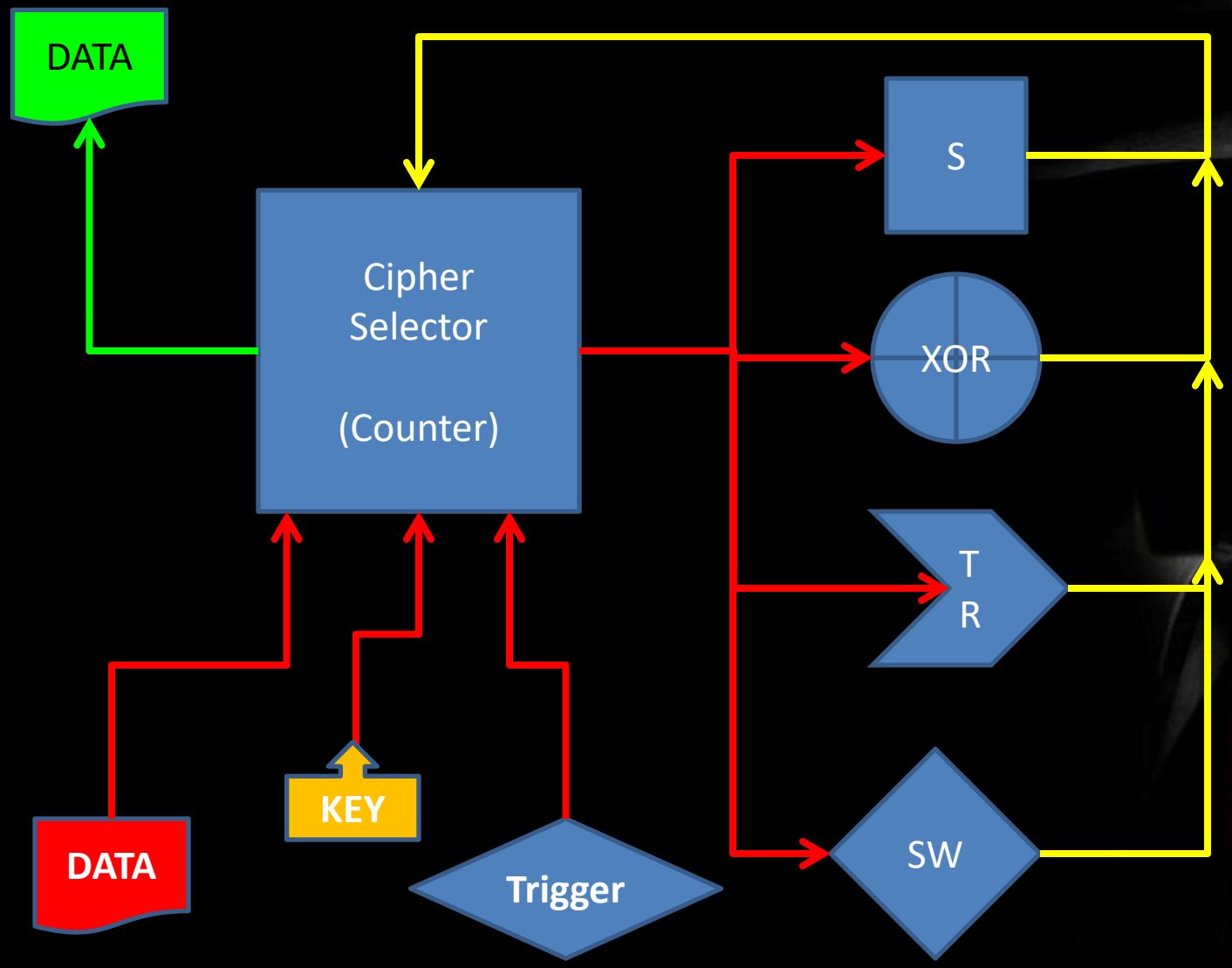
- Static (Cipher Never Changes)
- Reversible (Reverse Engineering)
- One Shoe Fits All

MEANS CURRENT SOFTWARE/HARDWARE IMPLEMENTATION OF CIPHERS

Randomized Ciphers Encryption



Randomized Ciphers Decryption



Benefits!!

- Inherently Random
- Reusable
- Abstraction
- Users Current Cipher Primitives
- Possible to replicate other Ciphers without changing code

Demo