

Randomized Ciphers

Security in Pure Process Abstraction

By Michael Kangethe and Chrispus Kamau

```
push edi
call sub_314623
test eax, eax
ja short loc_31306D
cmp [ebp+arg_0], ebx
jnx short loc_313066
mov eax, [ebp+var_70]
cmp eax, [ebp+var_84]
jb short loc_313066
sub eax, [ebp+var_84]
push esi
push esi
push eax
push edi
mov [ebp+arg_0], eax
call sub_31486A
test eax, eax
ja short loc_31306D
push esi
lea eax, [ebp+arg_0]
push eax
mov esi, 100h
push esi
push [ebp+arg_4]
push edi
call sub_314623
test eax, eax
ja short loc_31306D
loc_313066: ; CODE XREF: sub_312FD8+4E
; sub_312FD8+85
push 6Dh
call sub_31444F
loc_31306D: ; CODE XREF: sub_312FD8+2D
; sub_312FD8+49
sub_3140F3
test eax, eax
jg short loc_31307D
call sub_3140F3
jmp short loc_31308C
/
loc_31307D: ; CODE XREF: sub_312FD8+9C
call sub_3140F3
loc_31308C:
loc_31308F:
```

AfricaHackOn 2016



**AFRICA
HACKON**
INFOSEC RE-IGNITED

who_are_we

- Michael Kangethe
Infosec Enthusiast and Researcher
- Bsc IT, Msc Computer Science
- Interests:
 - Artificial Intelligence
 - Secure Data Communications
 - Dynamic Cryptosystems

```
push edi
call sub_314623
test eax, eax
ja short loc_31306D
cmp [ebp+arg_0], ebx
jnx short loc_313066
mov eax, [ebp+var_70]
cmp eax, [ebp+var_84]
jb short loc_313066
sub eax, [ebp+var_84]
push esi
push esi
push eax
push edi
mov [ebp+arg_0], eax
call sub_31486A
test eax, eax
ja short loc_31306D
push esi
push [ebp+arg_0]
mov esi, 100h
push esi
push [ebp+arg_4]
push edi
call sub_314623
test eax, eax
ja short loc_31306D
cmp [ebp+arg_0], esi
ja short loc_31308F

loc_313066: ; CODE XREF: sub_312FD8+4E
; sub_312FD8+55
push 0Dh
call sub_31444B

loc_31306D: ; CODE XREF: sub_312FD8+2D
; sub_312FD8+49
call sub_3140F3
test eax, eax
jg short loc_31307D
call sub_3140F3
jmp short loc_31308C

loc_31307D: ; CODE XREF: sub_312FD8+9C
call sub_3140F3
and eax, 0FFFFFFh
or eax, 80070000h

loc_31308C: ; CODE XREF: sub_312FD8+A3
mov [ebp+var_4], eax

loc_31308F: ; CODE XREF: sub_312FD8+8C
cmp edi, 0FFFFFFFh
ja short loc_31309A
push edi
```

who_are_we

- Crispus Kamau
Information Security Engineer
- Bsc Electrical and Electronics
- Interests:
 - Radio Frequency
 - Electronics/hardware
 - Mobile device security

```
push edi
call sub_314623
test eax, eax
ja short loc_31306D
cmp [ebp+arg_0], ebx
jnx short loc_313066
mov eax, [ebp+var_70]
cmp eax, [ebp+var_84]
jb short loc_313066
sub eax, [ebp+var_84]
push esi
push esi
push eax
push edi
mov [ebp+arg_0], eax
call sub_31486A
test eax, eax
ja short loc_31306D
push esi
mov eax, [ebp+arg_0]
push eax
mov esi, 100h
push esi
push [ebp+arg_4]
push edi
call sub_314623
test eax, eax
ja short loc_31306D
cmp [ebp+arg_0], esi
ja short loc_31308F

loc_313066: ; CODE XREF: sub_312FD8+4E
; sub_312FD8+65
push 6Dh
call sub_31444B

loc_31306D: ; CODE XREF: sub_312FD8+2D
; sub_312FD8+49
call sub_3140F3
test eax, eax
jg short loc_31307D
call sub_3140F3
jmp short loc_31308C

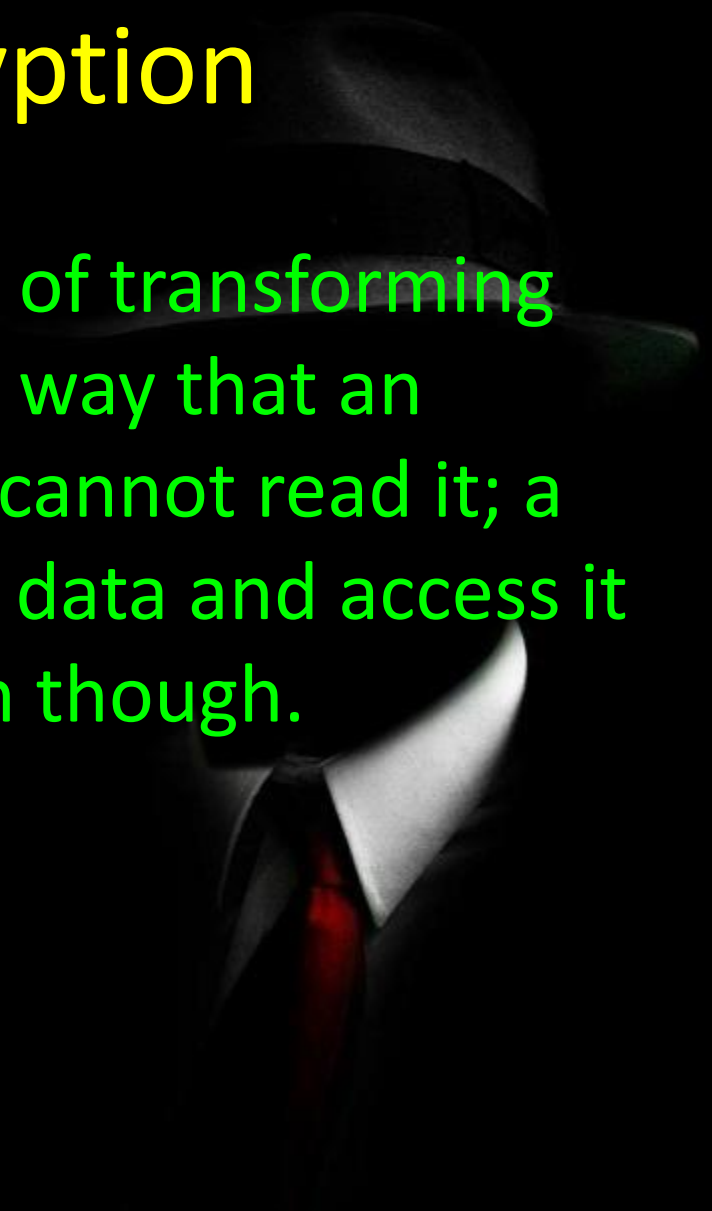
loc_31307D: ; CODE XREF: sub_312FD8+9C
call sub_3140F3
and eax, 0FFFFFFh
or eax, 80070000h

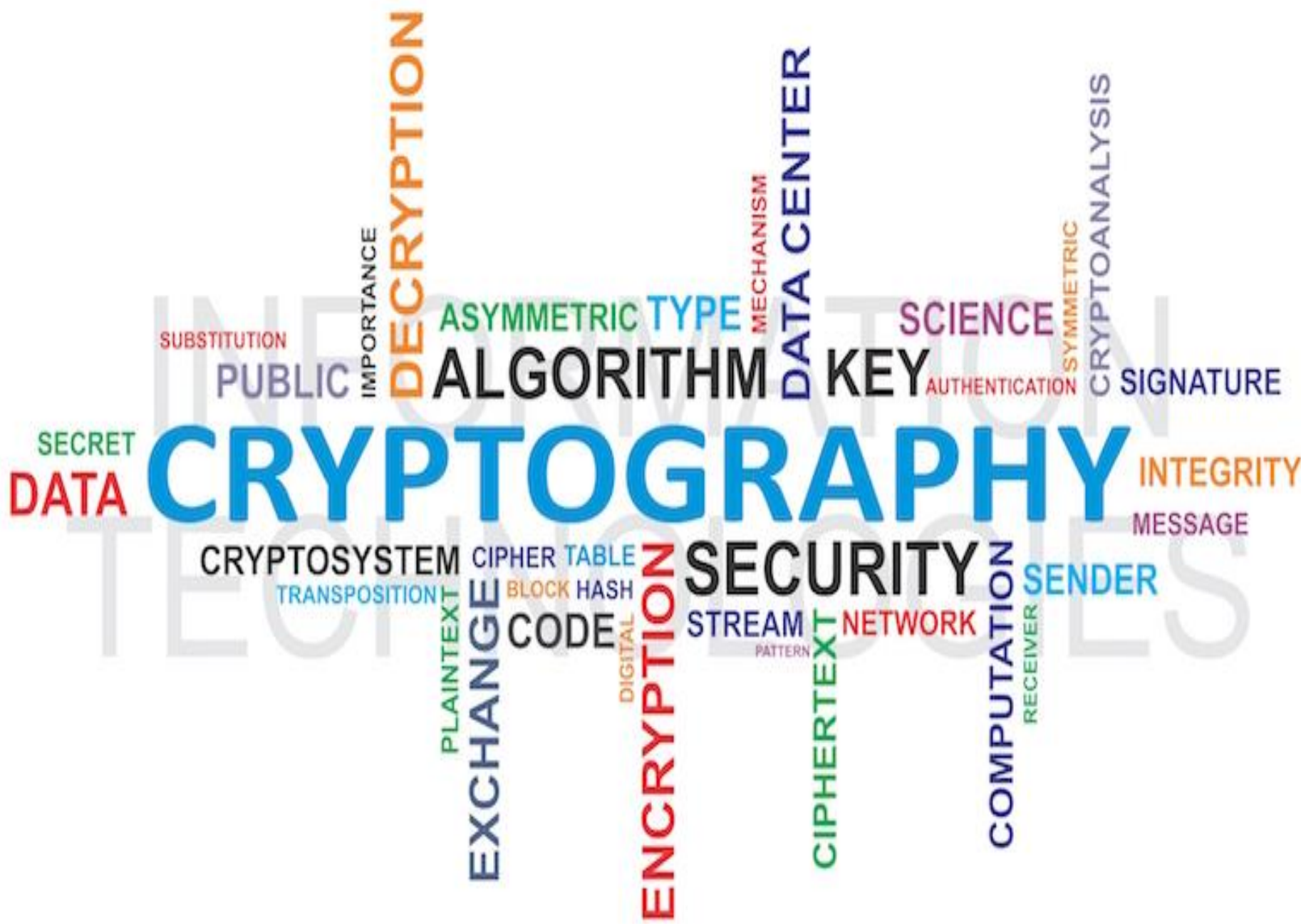
loc_31308C: ; CODE XREF: sub_312FD8+A3
mov [ebp+var_4], eax

loc_31308F: ; CODE XREF: sub_312FD8+8C
cmp edi, 0FFFFFFFh
ja short loc_31309A
push edi
```

What is Encryption

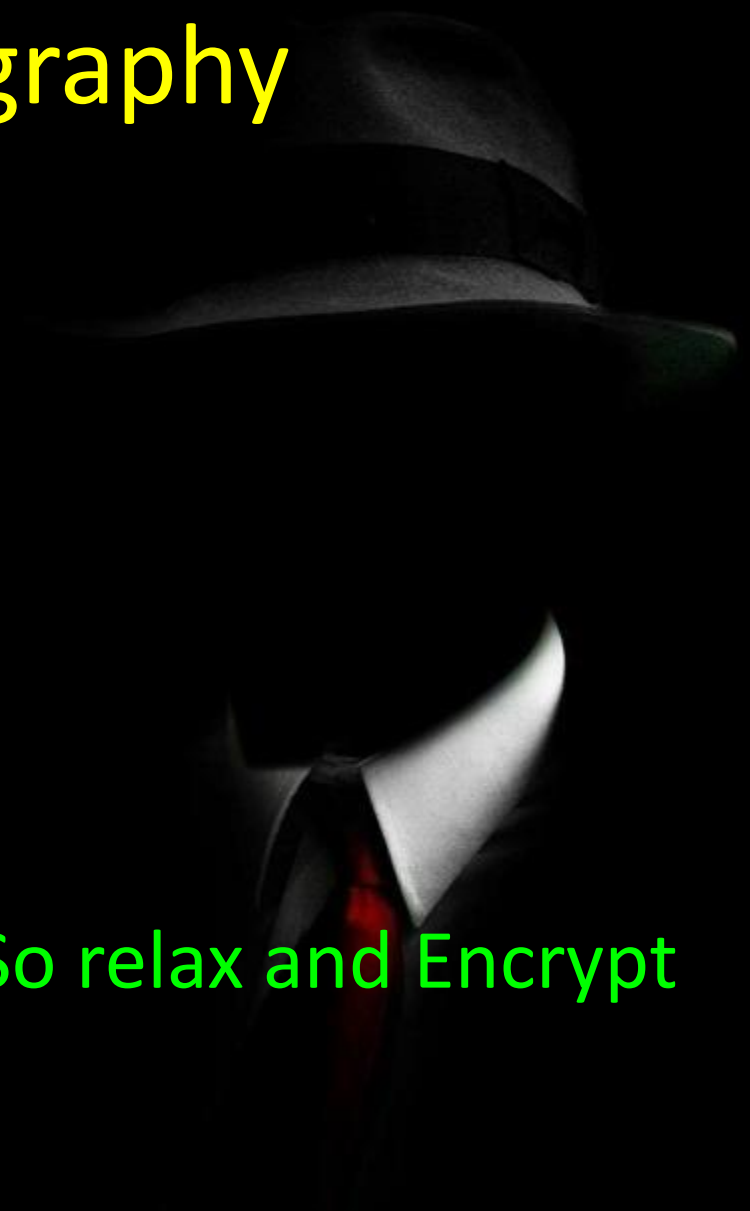
- Encryption is the process of transforming information in such a way that an unauthorized third party cannot read it; a trusted person can decrypt data and access it in its original form though.



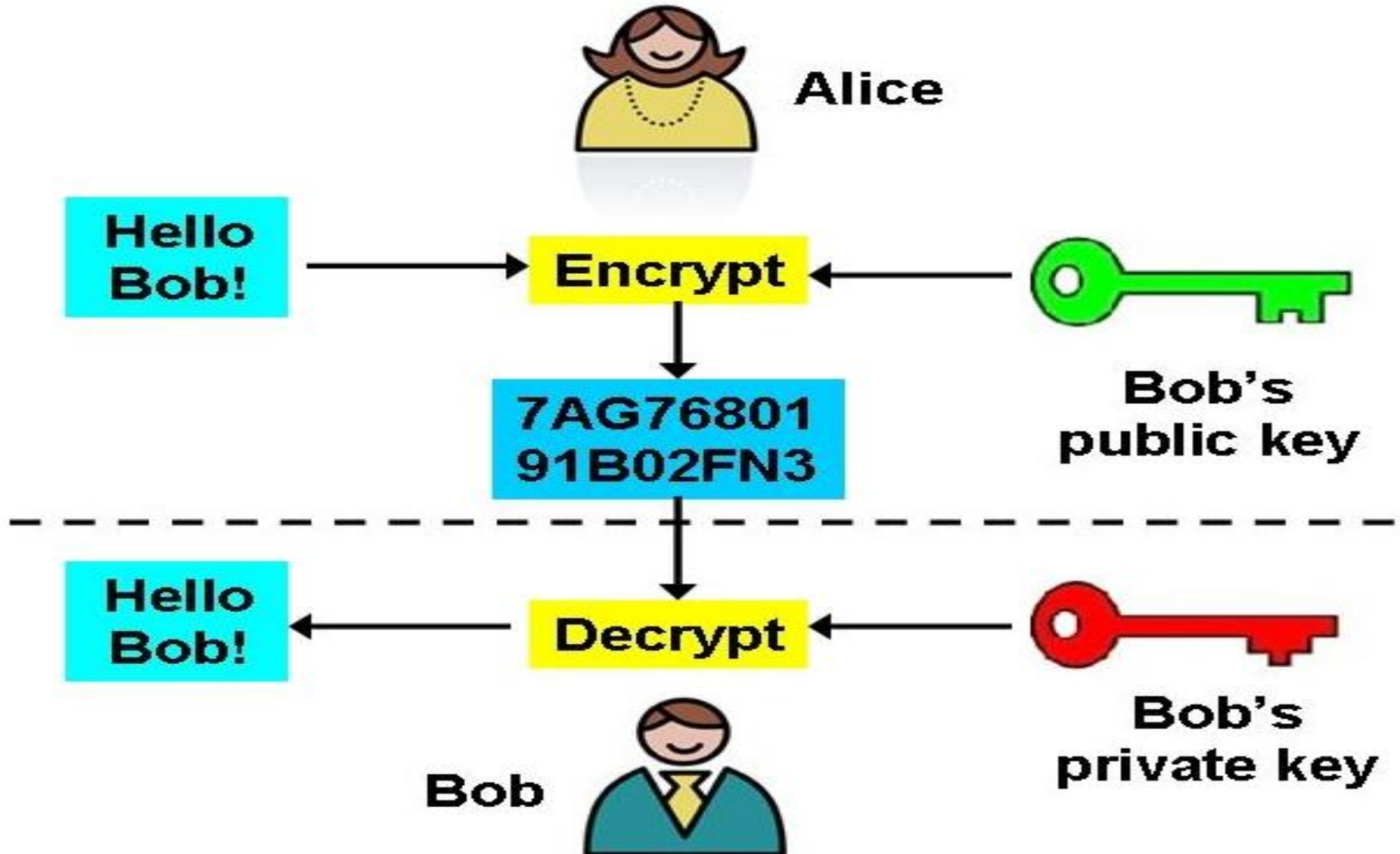


Why Cryptography

- 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

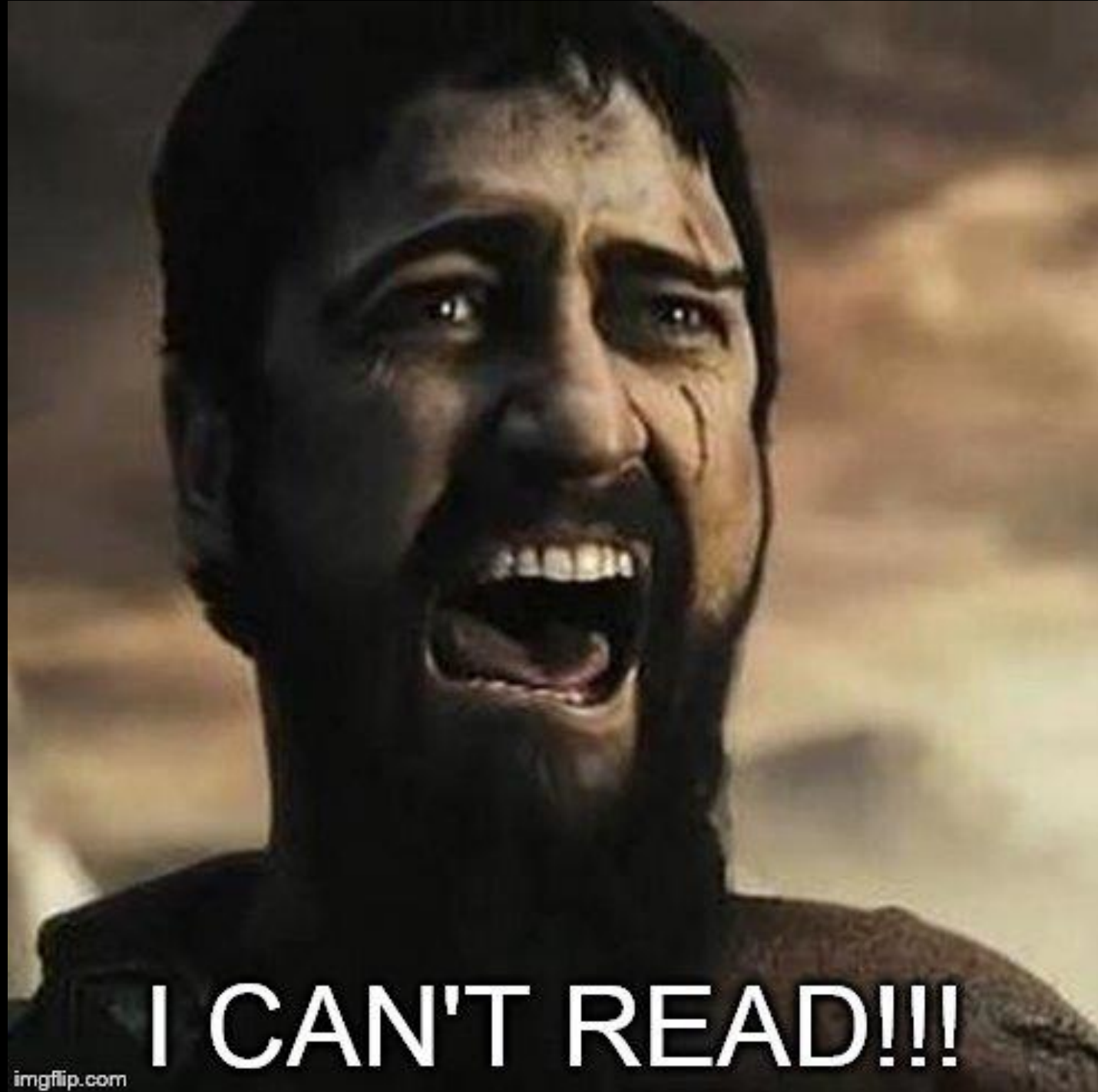
Dear Tim,....please find our revenues and profit statement for the last business year attached. This is confidential information.....Best regards.■

0stkgNGafvEYc3V
w1JDkv4PVJ+Lk1H
FhSmZgQ2hcjtFF1
ZvkoFu+y3fAUd4L
N/q6TrR8YSnL81F
idsi16CrN7nMAgB
36mBVL2gL4hYYGh
C+z06K+6PJ1WEZX
tMONYqZj3PE1whz
8UIZCUsCpnEB

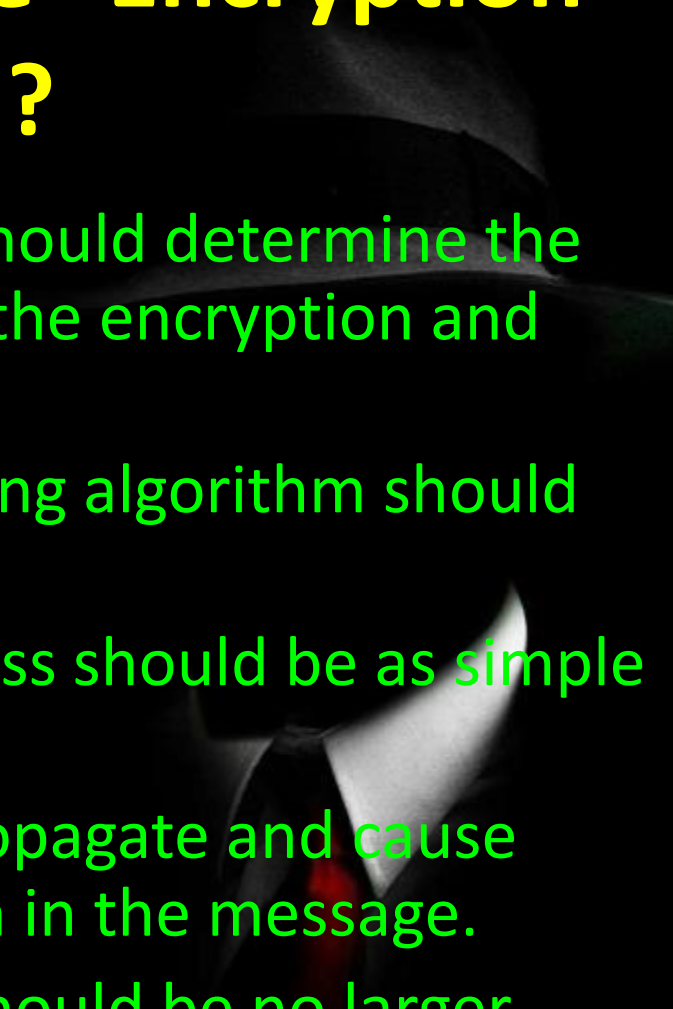
Preferred Reaction

WEH!





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



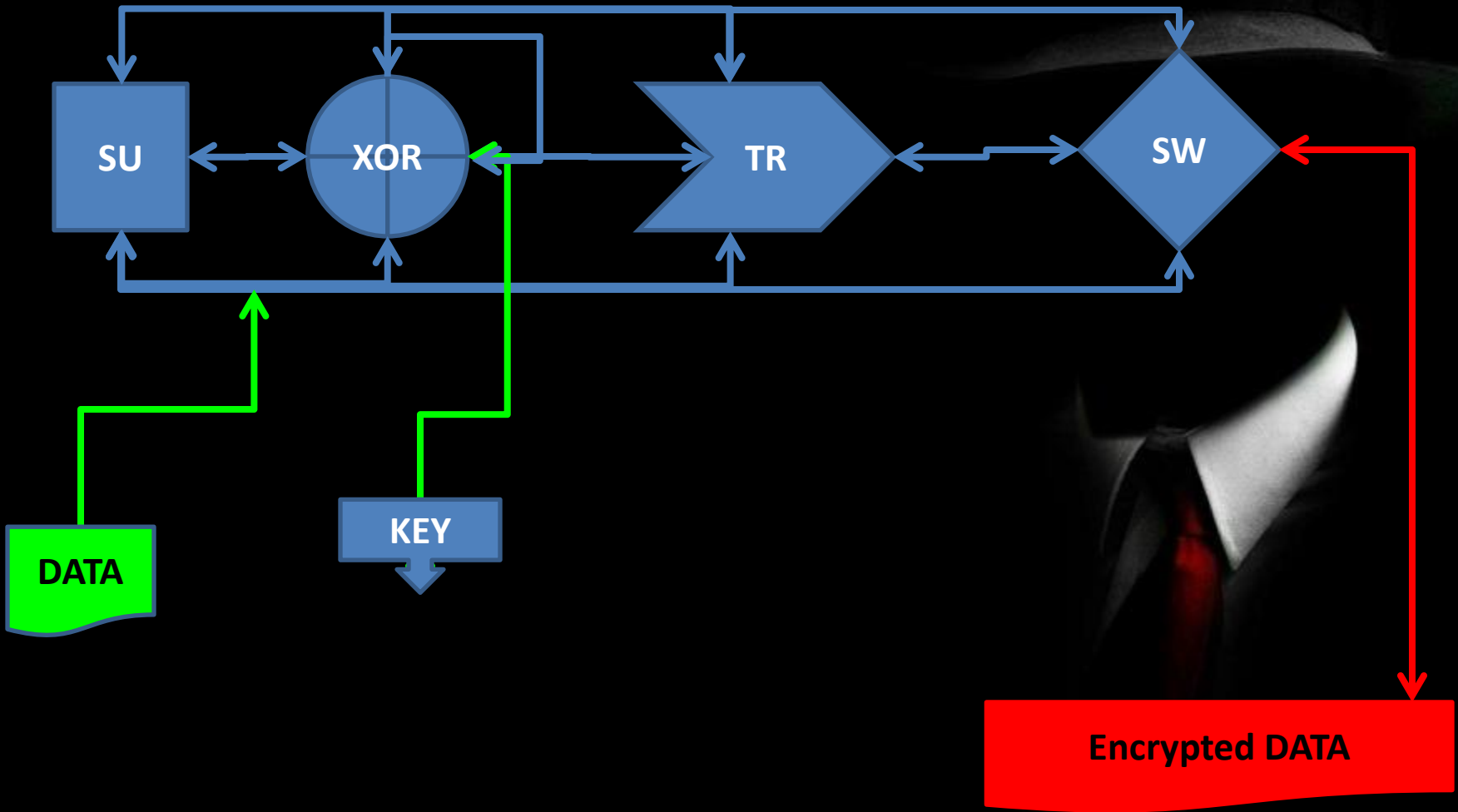
Switching bits



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

```
push edi
call sub_314623
test eax, eax
ja short loc_31306D
cmp [ebp+arg_0], ebx
jnz short loc_313066
push esi
push eax
push eax
sub eax, [ebp+var_54]
push esi
push esi
push eax
push edi
mov [ebp+arg_0], eax
call sub_31486A
test eax, eax
ja short loc_31306D
push esi
push esi
push esi
mov esi, 100h
push esi
push edi
call sub_314623
jnz short loc_31306D
cmp [ebp+arg_0], esi
ja short loc_313085
loc_313066: ; CODE XREF: sub_312FD8+4E
; sub_312FD8+55
push 6Dh
call sub_31444B
loc_31306D: ; CODE XREF: sub_312FD8+2D
; sub_312FD8+49
call sub_3140F3
test eax, eax
jg short loc_31307D
call sub_3140F3
jmp short loc_31308C
;
loc_31307D: ; CODE XREF: sub_312FD8+9C
call sub_3140F3
and eax, 0FFFFFFh
or eax, 80070000h
loc_31308C: ; CODE XREF: sub_312FD8+A3
mov [ebp+var_4], eax
loc_31308F: ; CODE XREF: sub_312FD8+8C
cmp edi, 0FFFFFFFh
ja short loc_31309A
push edi
```

A CRYPTO NERD'S IMAGINATION:

HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.

NO GOOD! IT'S 4096-BIT RSA!

BLAST! OUR EVIL PLAN IS FOILED!



WHAT WOULD ACTUALLY HAPPEN:

HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS \$5 WRENCH UNTIL HE TELLS US THE PASSWORD.



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



RETWEET
1



PM - 8 Feb 2016

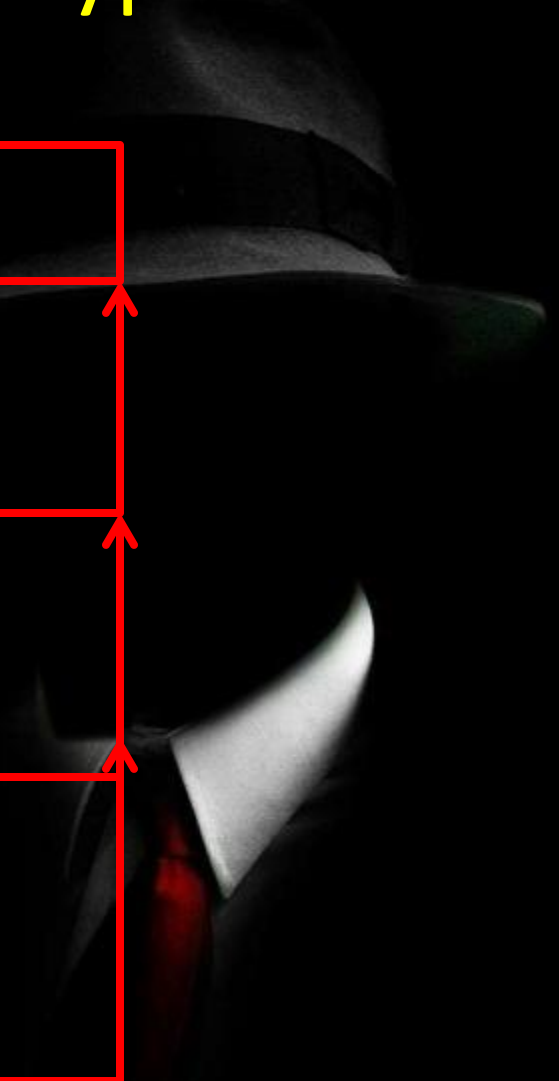
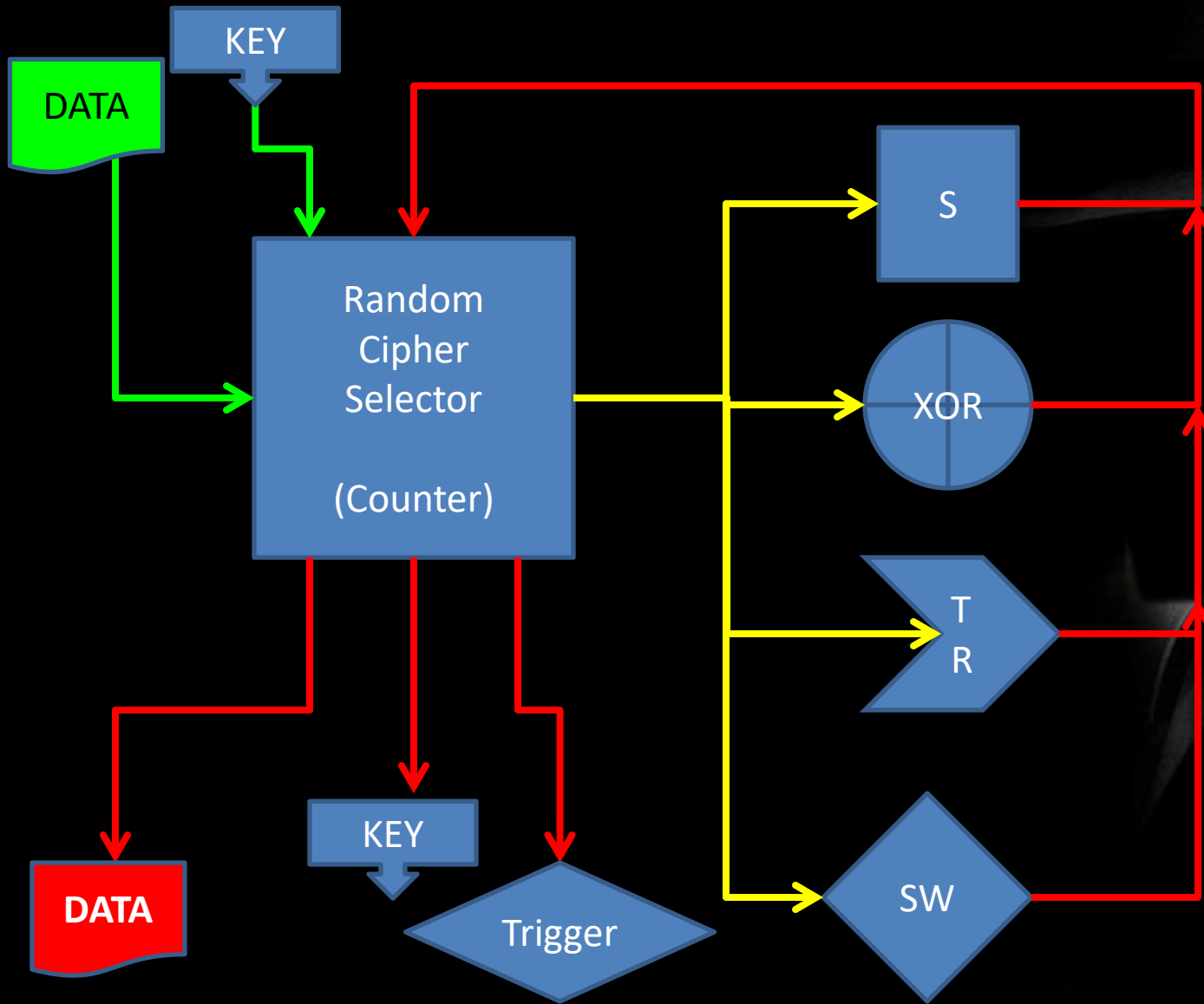
Facts (Current Cryptosystems)

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

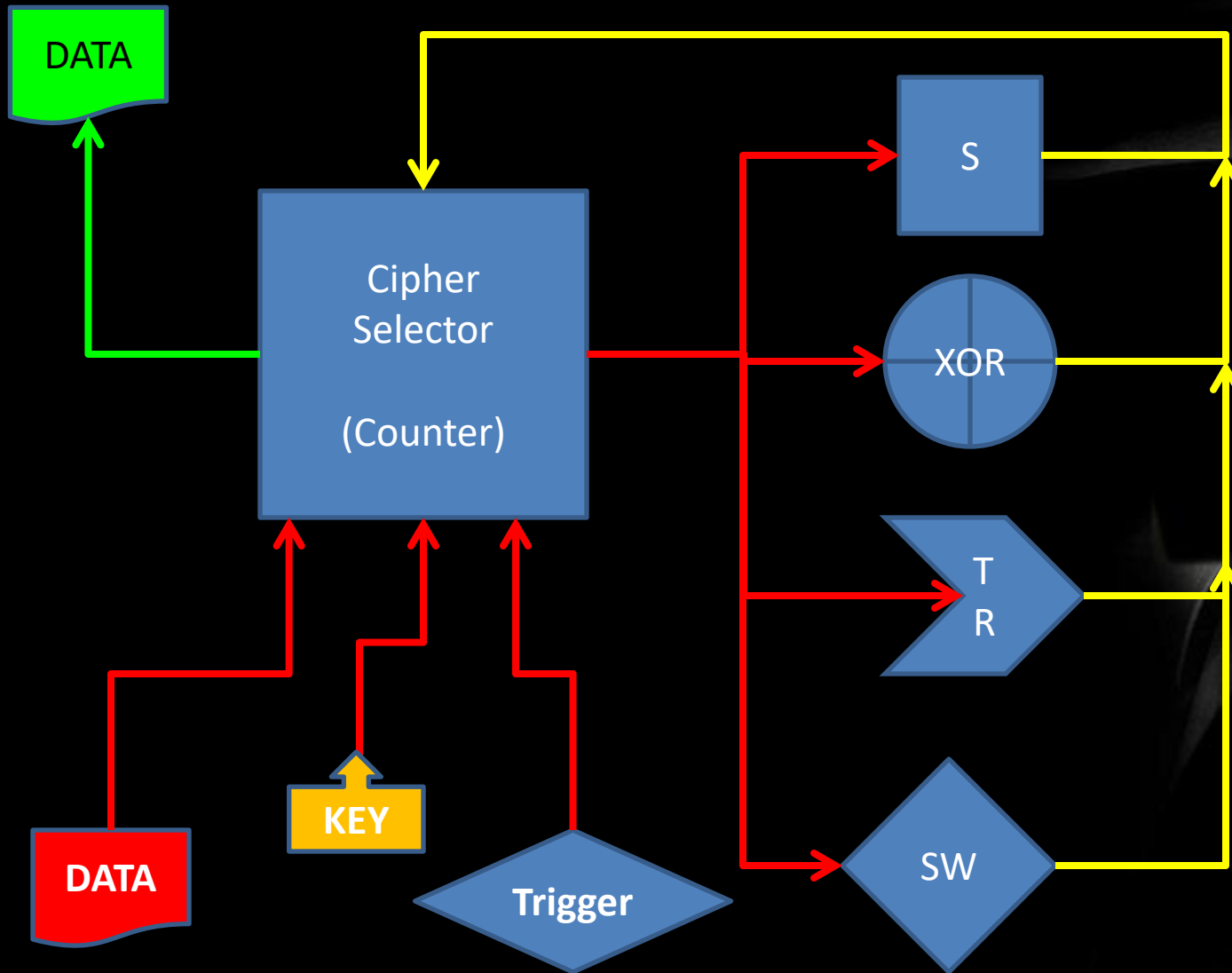
**MEANS CURRENT SOFTWARE/HARDWARE
IMPLEMENTATION OF CIPHERS**



Randomized Ciphers Encryption



Randomized Ciphers Decryption



Benefits!!

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



Demo

