Hacking The Planet: Intro to Avionics Security

By Caitlin Long @0x26d

About me:

Hi, I’m Caitlin! I’ve been working in infosec for nearly 2 years now, and my hobbies/interests include aerospace and computer security.

One of my plans after the pandemic ends is to finally take flying lessons!

What this talk will be about!

In this talk, I’ll be talking the security and cryptography of the on board embedded computer systems on aircraft, and what side channel attacks, and hardware security.

Large aerospace companies have engineers dedicated to this complex type of hardware security.

Vocabulary!

Avionics by definition are the electronic systems used on aircraft, artificial satellites, and spacecraft.

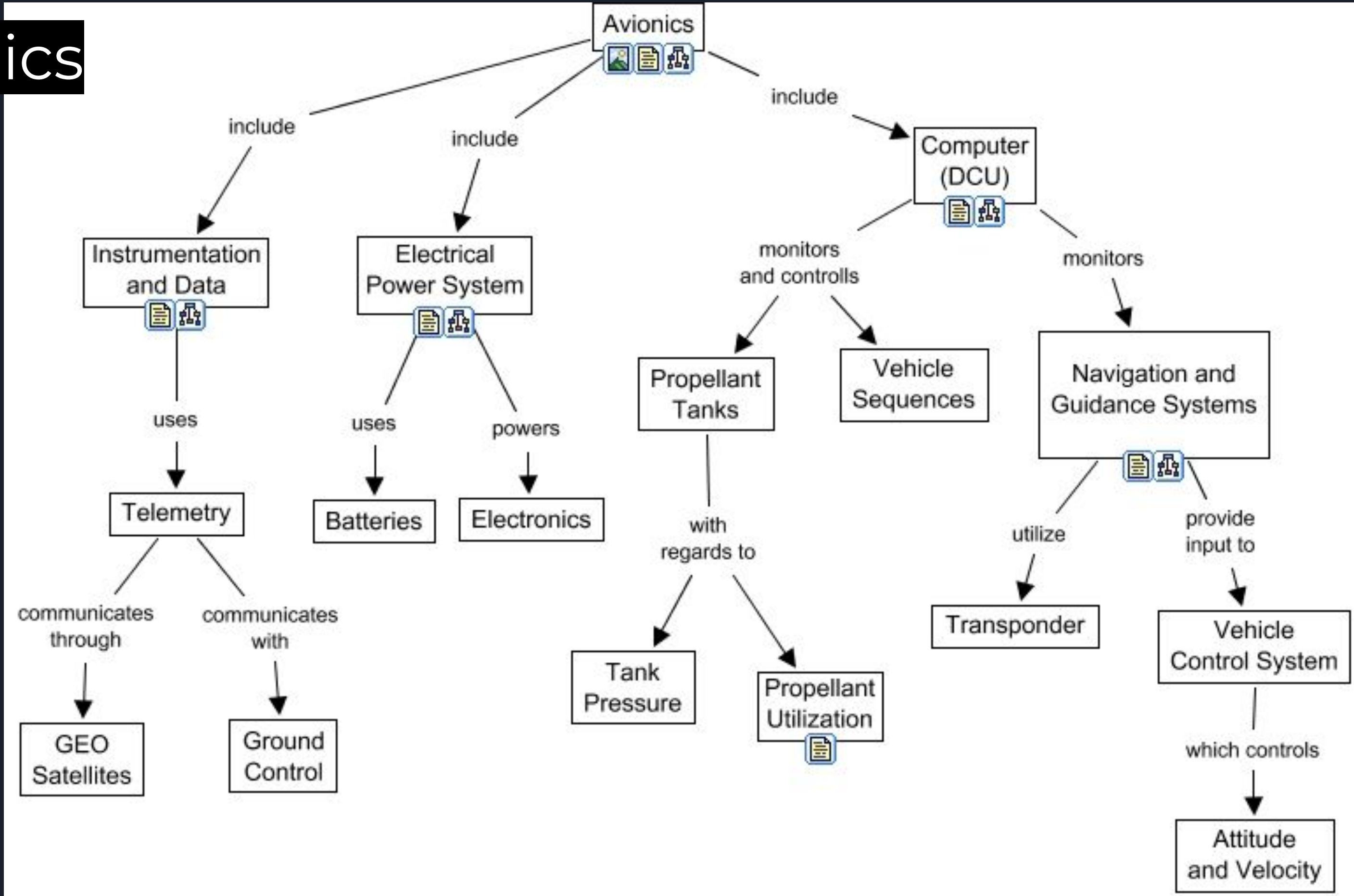
Cryptosystems are defined as a pair of algorithms that do encryption and decryption based on a key.

Side channel attacks are defined as attacks based on information gained from the implementation of a computer system, to derive the secret key.

Intro to Avionics

Different types include communications, navigation, monitoring, flight control systems, and management systems.

DCU stands for Data Concentrator Unit.



Intro to cryptography (my favorite!)

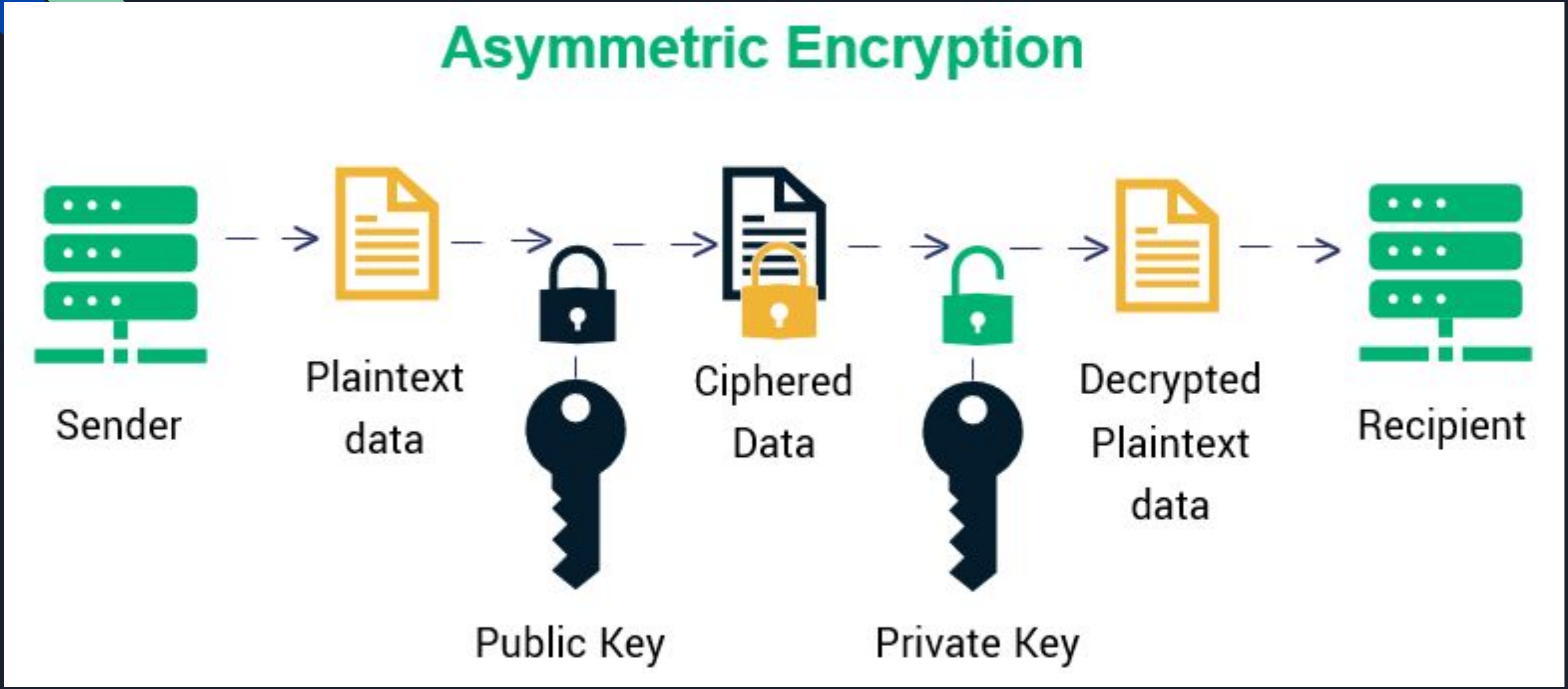
Cryptography, in its simplest form, can be described as a way of encoding and decoding messages.

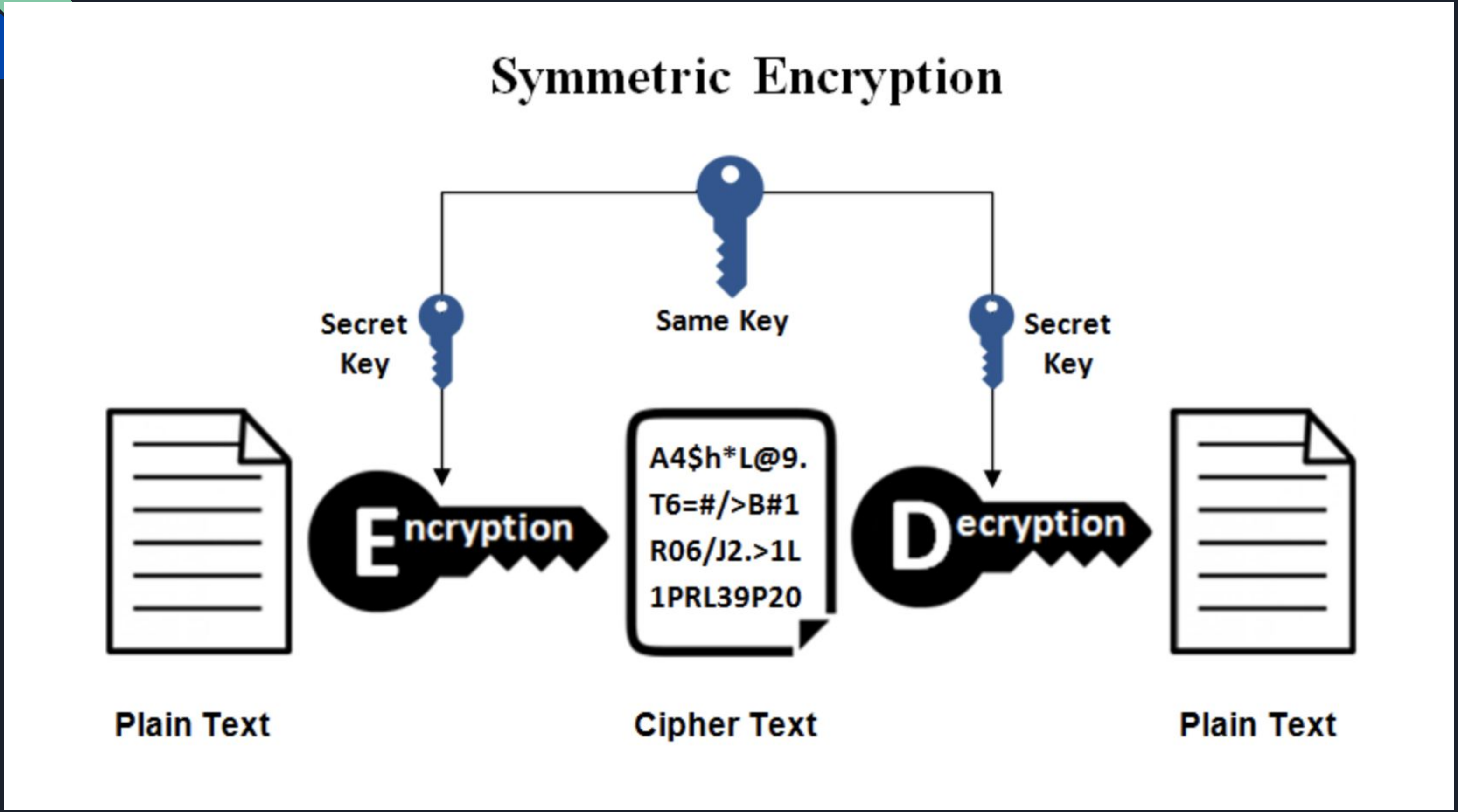
2 algorithm types: symmetric and public key.

Several types of cryptographic attacks, including password cracking (brute force, rainbow table, dictionary attack), collision attack, birthday attack, and many more.

Picture is of Alan Turing, known for cracking Nazi enigma machines during WW2 and for creating the foundation of theoretical computer science.

Asymmetric cryptography (public key)

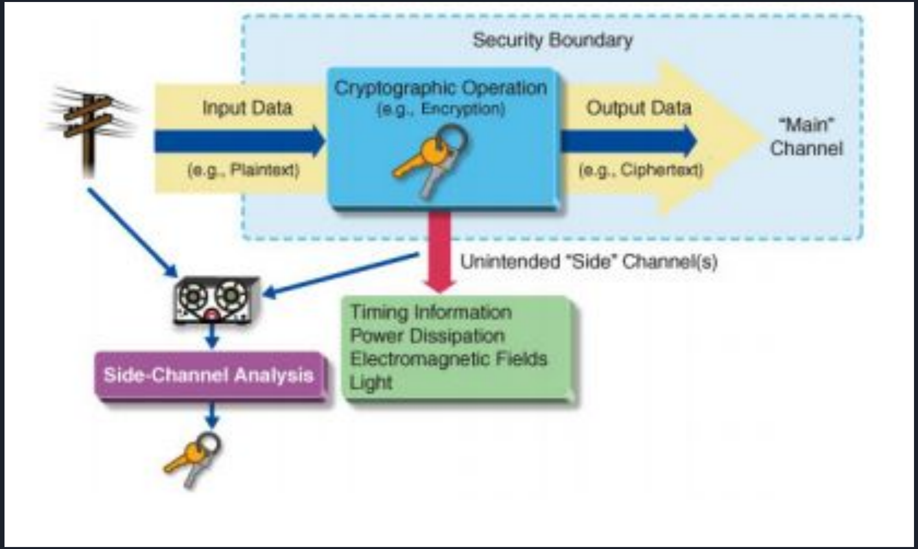


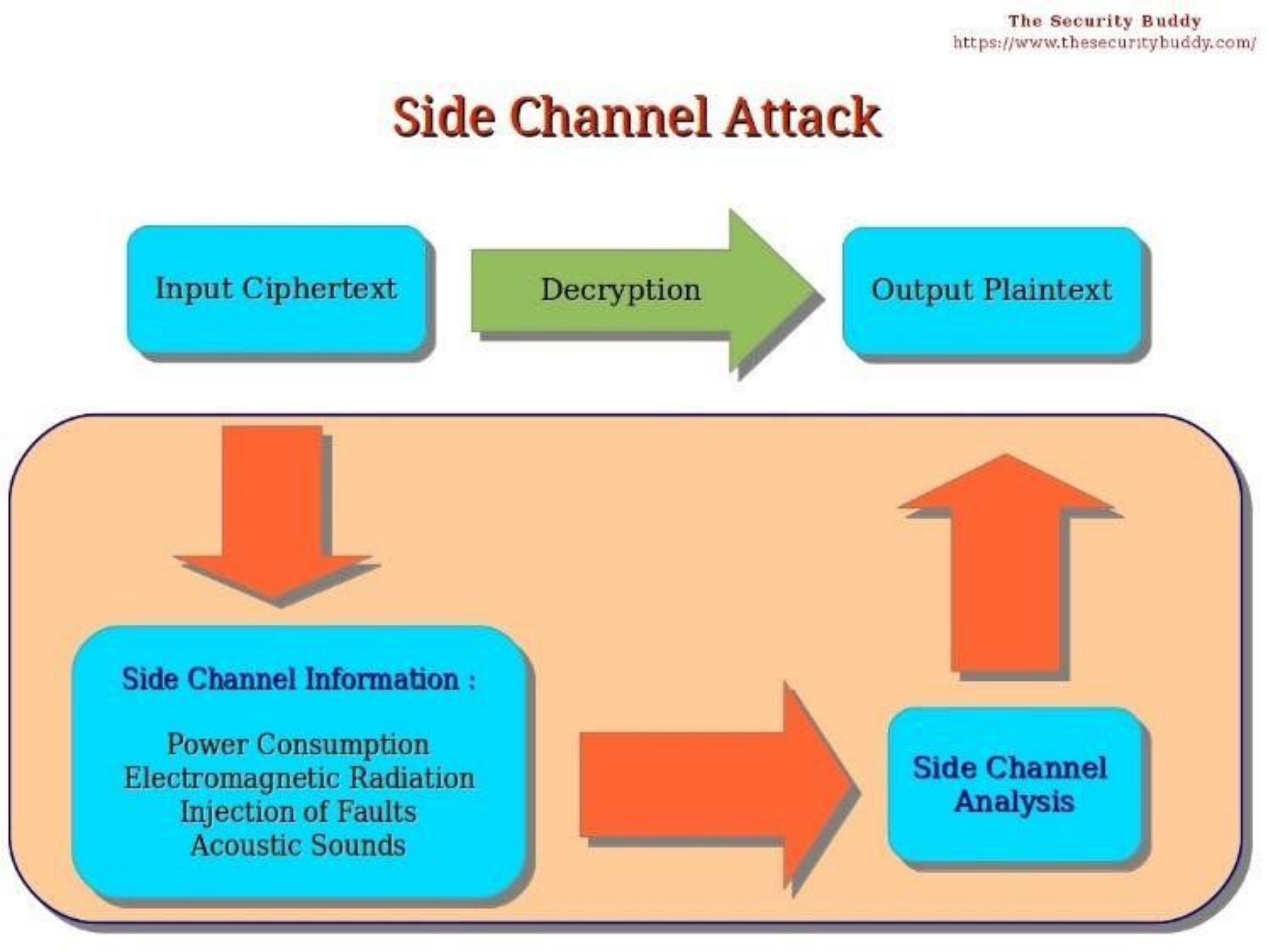

Symmetric Encryption
Secret Key
Same Key
Secret Key
Encryption
A4$h*L@9.
T6=#/>B#1
R06/J2.>1L
1PRL39P20
Decryption
Plain Text
Cipher Text
Plain Text

Side channel attacks

Side channel attacks are hardware cryptanalytic attacks that exploit the physical behavior of a system, such as timing, power consumption, and electromagnetic emissions.

Other types of attacks include power analysis.





The Security Buddy
https://www.thesecuritybuddy.com/

Side Channel Attack

Input Ciphertext

Decryption

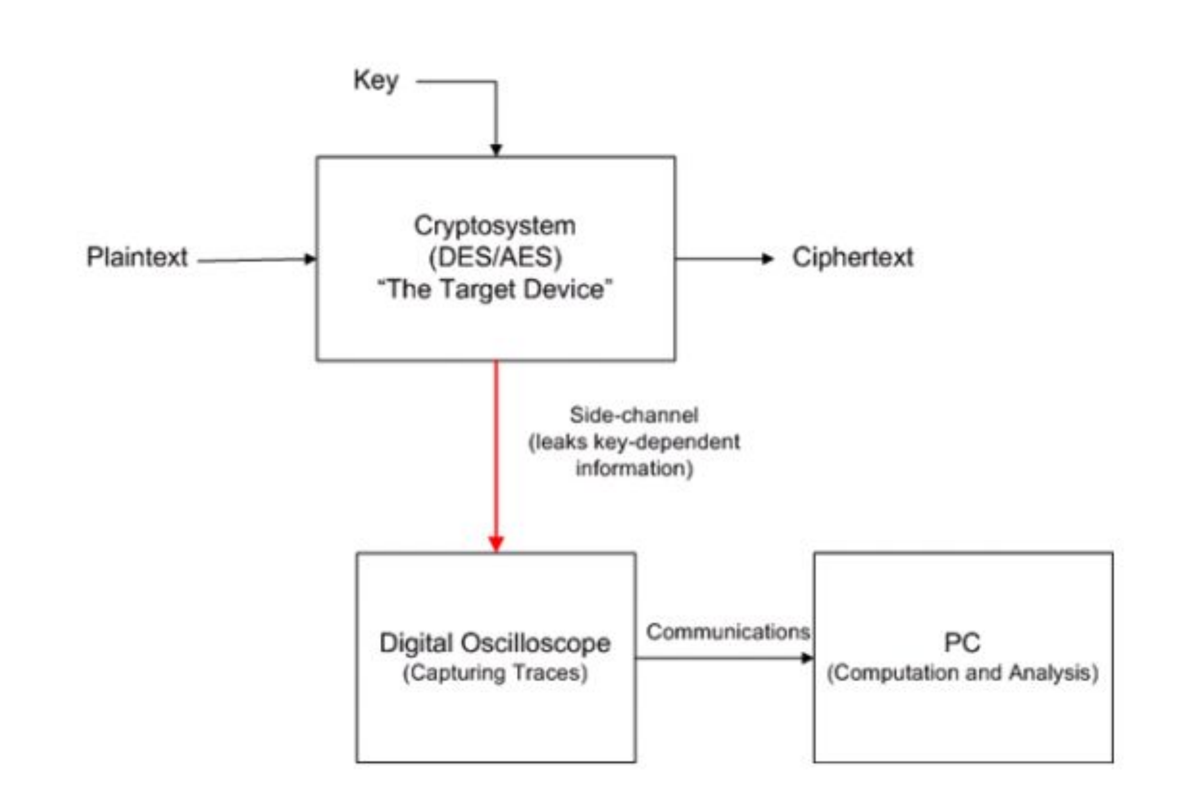
Output Plaintext

Side Channel Information :

Power Consumption
Electromagnetic Radiation
Injection of Faults
Acoustic Sounds

Side Channel Analysis

Attacks are performed with an oscilloscope & computer


Key
Plaintext
Cryptosystem (DES/AES) "The Target Device"
Ciphertext
Side-channel (leaks key-dependent information)
Digital Oscilloscope (Capturing Traces)
Communications
PC (Computation and Analysis)

Power analysis attacks

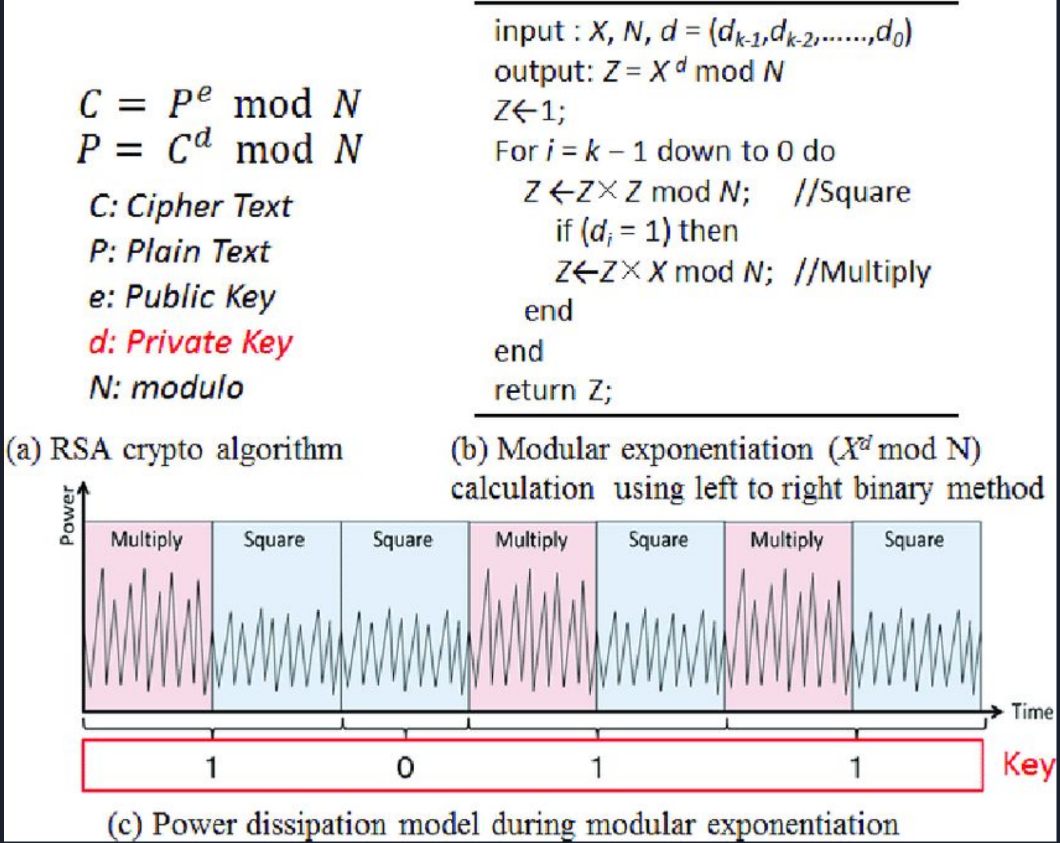
These attacks are done by examining the power consumed by a device running public key cryptographic algorithms over time.

2 main ones: simple and differential.

Simple Power Analysis

SPA recovers a key from a single crypto transaction. Requires a strong signal, close proximity to target device, and is usually applied to public key cryptography based systems.

SPA can reveal sequence of instructions executed by a machine.



$$C = P^e \mod N$$
$$P = C^d \mod N$$

C: Cipher Text

P: Plain Text

e: Public Key

d: Private Key

N: modulo

```
input : $X, N, d = (d_{k-1}, d_{k-2}, \ldots\ldots, d_0)$
output: $Z = X^d \bmod N$
$Z \leftarrow 1$;
For $i = k - 1$ down to 0 do
    $Z \leftarrow Z \times Z \bmod N$;     //Square
      if ($d_i = 1$) then
      $Z \leftarrow Z \times X \bmod N$;  //Multiply
    end
end
return Z;
```

(a) RSA crypto algorithm

(b) Modular exponentiation (X^d mod N) calculation using left to right binary method

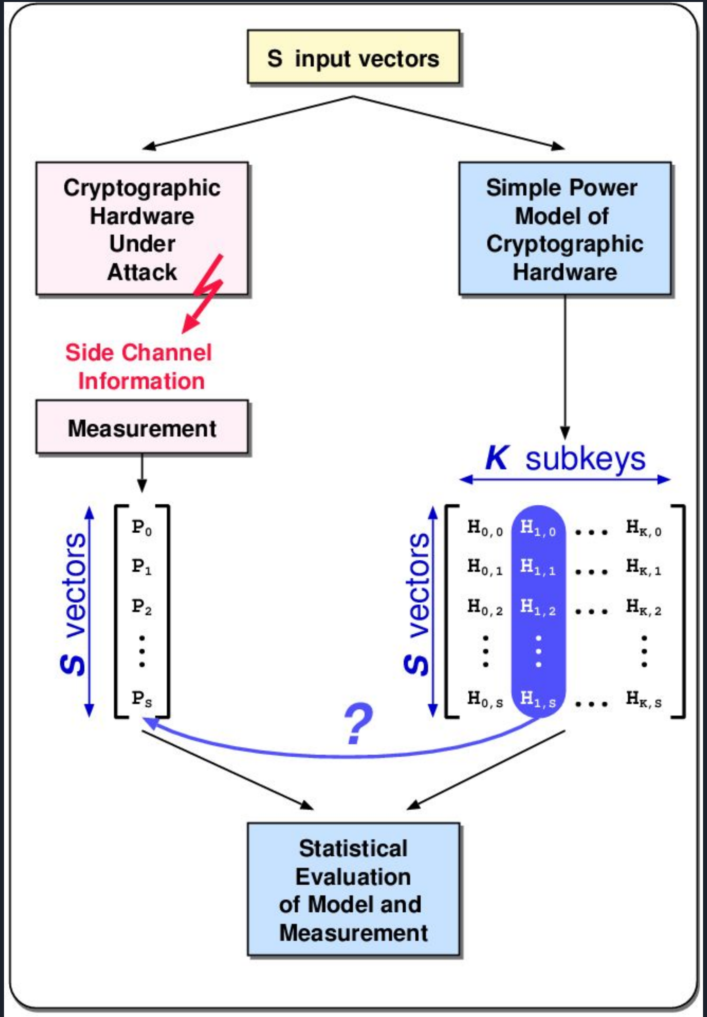
(c) Power dissipation model during modular exponentiation

SPA attack exploiting a power trace during modular exponentiation in RSA algorithm

Differential Power Analysis

DPA is a form of side-channel attack that monitors variations in the electrical power consumption or electromagnetic emissions of a target device.

DPA attacks are measure different parts of the chip to recover the key. DPA attacks are more powerful than SPA and harder to prevent.



Simple representation of the DPA attack.

for each one of the K subkey permutations, S samples are processed and the hypothetical power consumption $H_{1..K,1..S}$ is calculated.

Then the power consumption of the device is recorded while it processes the same S samples using the same unknown key

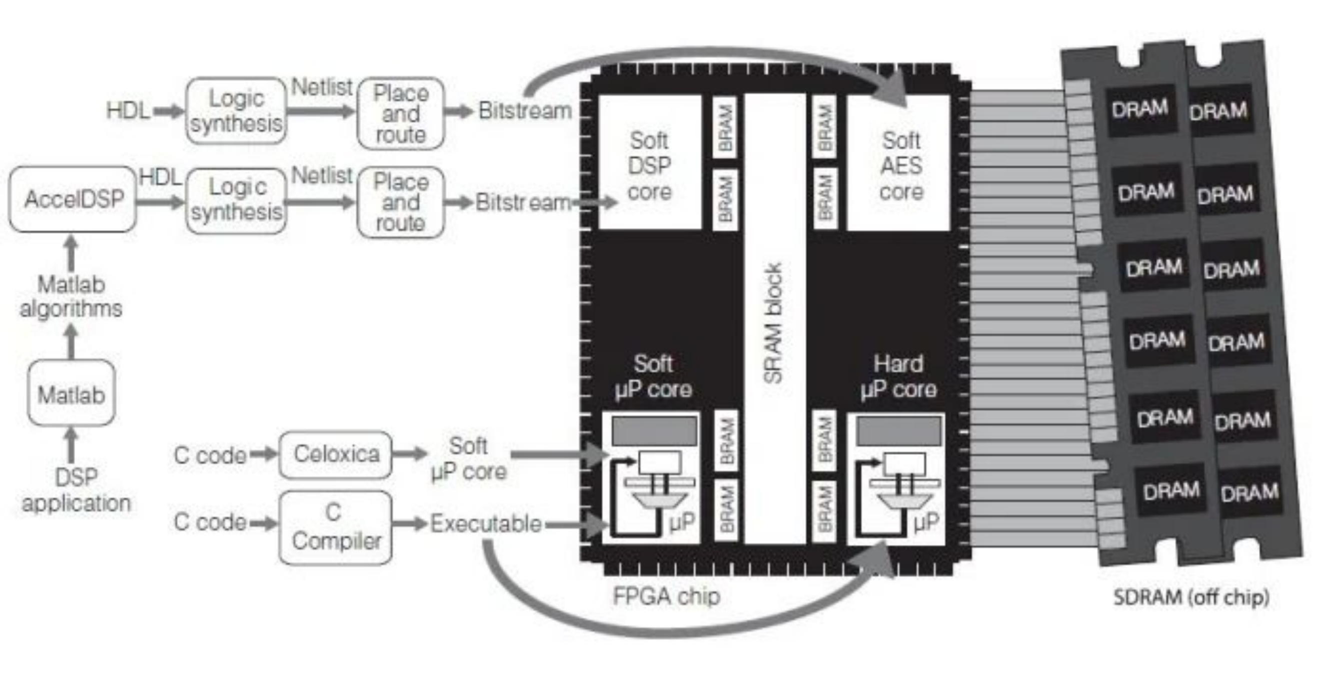
This leads to a vector $P_{1..S}$, holding the different power consumptions for all S inputs

The correct subkey is revealed by correlating the hypothetical power consumptions H1..K,1..S with the measured power consumptions P1..S.

In a successful attack, the correct subkey hypothesis Hkc,1..S will show a 'significantly' higher correlation to the measured power P1..S than all other subkey hypotheses.

Back to avionics!

FPGA - field programmable gate array.

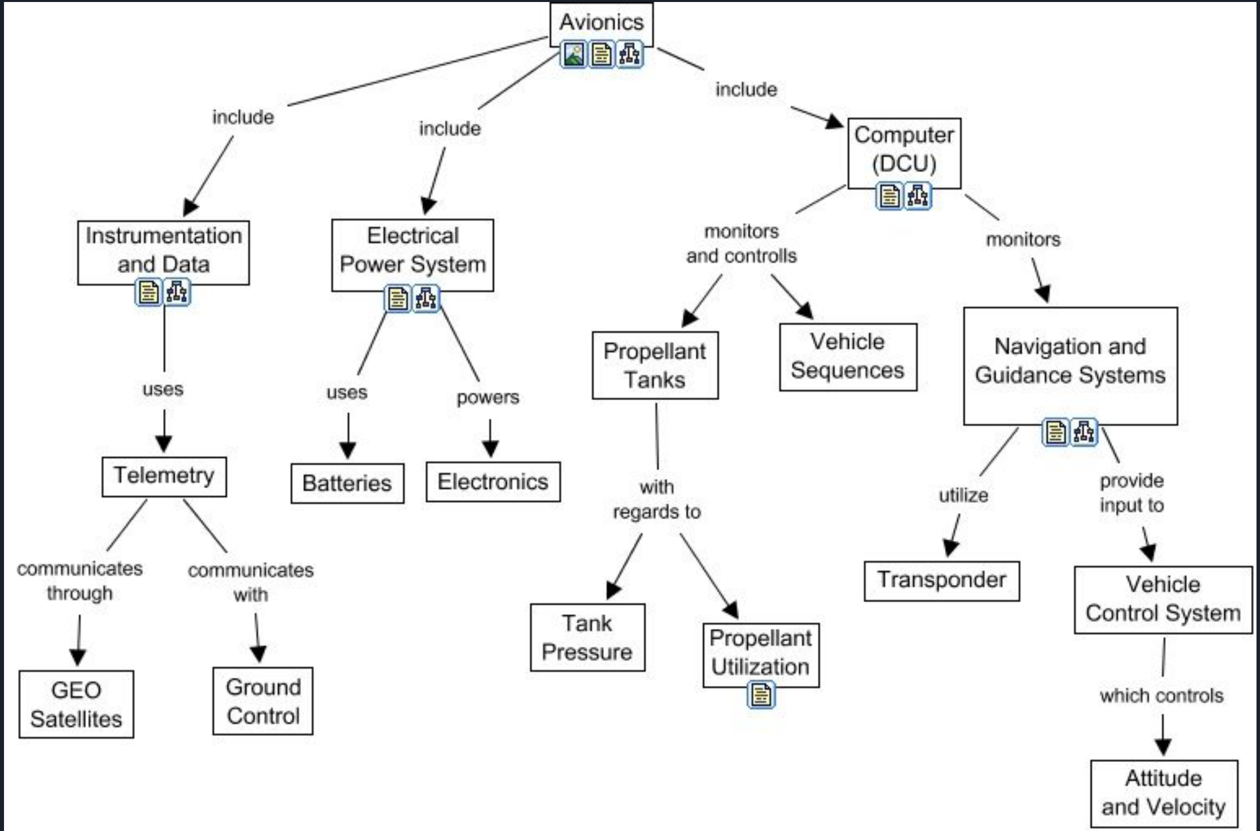


Moar on FPGA!

FPGAs are used in a variety of systems, such as **avionics**, encryption, intrusion detection systems, supercomputers and others applications.

These ICs (integrated circuits) are supposedly secure due to the code customization it allows for. Think of it as buying a plain frosted cake at the grocery and decorating it yourself.

FPGAs are the most commonly used chip in aerospace and span a wide array of applications in avionics.



FPGA chips are widely used across all aerospace and aircraft systems.

How does this relate to aerospace?

Big aerospace companies that do defense contracting often have software engineers that work on FPGA chips and on embedded cryptographic functions and systems.

I thought it was a cool field that no one knows about so I decided to do a talk on it :)

Twitter - @0x26d