Side Channel Attacks

A curious security break methodology

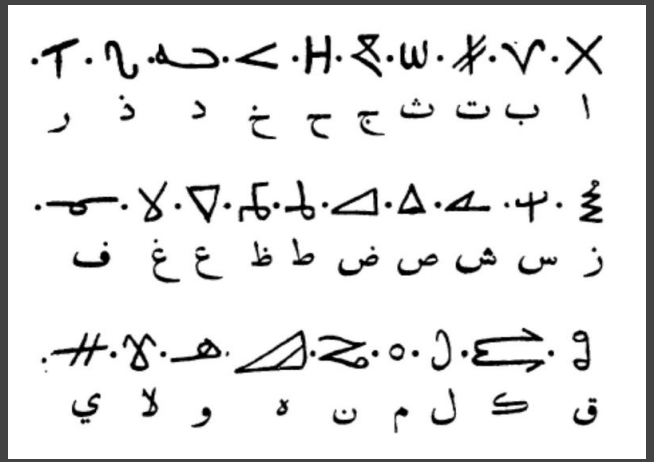
Alberto Serrano Ibaibarriaga
Miguel García Martín

Index

1. A bit of history

Cryptography has been around since at least 4.000 years ago; and, with it, cryptanalysis.

These two disciplines conform the field of cryptology.



2. Classical ciphers

Complicated algorithms are prone to errors (even easy ones are).

As the messages had to be encrypted by hand, the ciphers had to be kept simple:

- Substitutions:
  - Monoalphabetic substitutions (e.g.: "Caesar's cipher", roman cipher used by Julius Caesar and Augustus).
  - Polyalphabetic substitutions (e.g.: "Vigenère cipher", medieval cipher developed by a french diplomat).
- Transpositions:
  - Columnar transpositions (e.g.: "Übchi", german cipher from the WWI).
  - Grille-based transpositions (e.g.: "Cardan grille", medieval cipher developed by an Italian polymath).

2. Classical ciphers

Therefore, these methods are suitable of being broken by cryptanalysis by hand.

Only a few cipher machines were built at the beginning of the XXth century:

- Hagelin C-36
- Enigma
- Vernam cipher machine

3. Cryptanalysis

Cryptanalyst can use a great variety of techniques to try to break the cipher and get the cipher key (and, therefore, the plaintext messages).

Different scenarios:

- Ciphertext only attack: only the ciphertext is known.
- Chosen plaintext attack: The plaintext to be encrypted can be arbitrarily selected.
- Known plaintext attack: Subcase of a chosen plaintext attack. The original plaintext (or bits of it) is known.
- Chosen ciphertext attack: The ciphertext to be decrypted can be arbitrarily selected.

3. Cryptanalysis

Different techniques for every scenario:

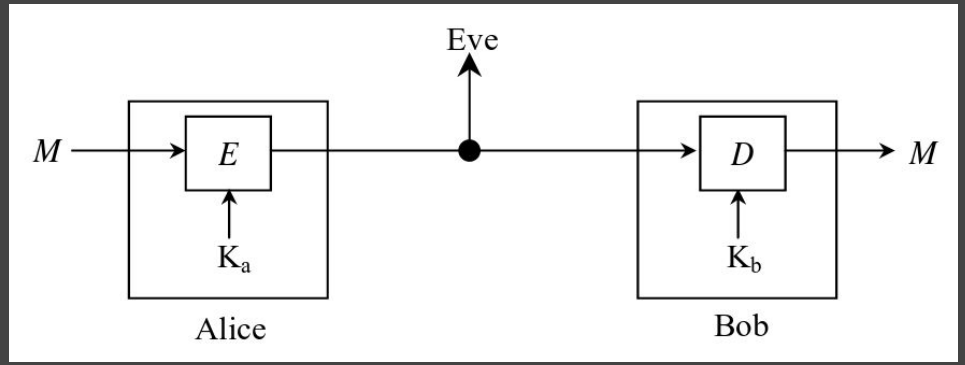
- Frequency analysis
- Chi and phi tests
- Kerckhoffs attack
- Kasiski examination
- And many more...

4. Modern ciphers

With the new available technology new algorithms were developed, as computers make calculations faster and without errors.

These algorithms are more complicated:

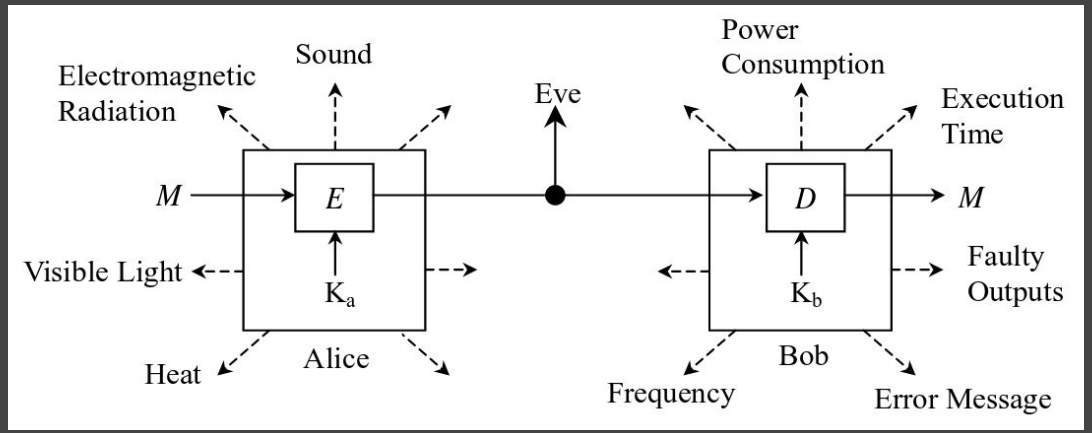
- RSA
- AES
- RC4



4. Modern ciphers

Old cryptanalysis techniques still can be done, but is much more difficult to do it by hand:

- Early versions of Microsoft's PPTP VPN used a cipher vulnerable to ciphertext-only attacks.
- RC4 is vulnerable to related-key attacks.



5. Side Channel Attacks

Even though the modern ciphers can still be cryptanalyzed, the use of computers to perform the encryption can also provide information about the process.

New attack vector: information leaked while computing.

- Timing attacks
- Power consumption
- Electromagnetic radiation
- Sounds made by the computer (vibrations, hard disks working...)
- Data remanence

These attacks target a concrete implementation of an algorithm.

6. Methods: Power Analysis Attack

These attacks use statistical analysis of the power consumed when performing different operations.

Example: consumption attack on RSA's modular exponentiation.

Equations of the *square and multiply* algorithm:

$$x^n = \begin{cases} x\,(x)^{\frac{n-1}{2}}, & \text{if } n \text{ is odd} \\ (x^2)^{\frac{n}{2}}, & \text{if } n \text{ is even} \end{cases}$$

6. Methods: Power Analysis Attack

An example in pseudocode to calculate M^e mod N.

The number of operations is proportional to the number of 1's on the exponent; so is power consumption.


```
function powModN (M, e, N): R
        var R ← 1, S ← M

        for i in bits do      {From 0 to n-1}

                if ((bit i of N) = 1) then
                        R ← R * S mod N
                end if

                S ← S^2 mod N
        end for

        return R
end function
```

7. Methods: Cache Attack

Based on the slower time spent when retrieving a value from cache instead of the main memory.

Example: Advanced Encryption Standard.

On AES, a set of lookup tables is used to decrease the time needed to encrypt.

The index used to get a value depends on the key. The system stores this values on cache, as they're often used → less time to access → key leaked.

8. Methods: Electromagnetic Attack

Attacks that take advantage of the electromagnetic radiation originated on the processor due to the magnetic field created by electrons moving through the connections.

Example: van Eck phreaking.

CRT (Cathode Ray Tube) and LCD monitors emit waves on the radio frequency that can be received and interpreted to draw the content of the first monitor on the second one (leaking any valuable information).

8. Methods: Electromagnetic Attack

This can be applied not only to screen content:

- TEMPEST:
  - NSA's codename for the radiation-related attacks (later an specification for spying and shielding techniques; and also NATO certification).
  - Many specifications are classified.
  - During WWII, while using a 131-B2 cipher machine, a near oscilloscope detected the encryption of each letter, allowing any eavesdropper to read the plaintext.

9. Bibliography

David Kahn, The codebreakers - ISBN: 978-0-684-83130-5

Cache-timing attacks on AES:
https://cr.yp.to/antiforgery/cachetiming-20050414.pdf

A Cache Timing Attack on AES in Virtualization Environments:
http://fc12.ifca.ai/pre-proceedings/paper_70.pdf

Side channel attacks:
http://gauss.ececs.uc.edu/Courses/c653/lectures/SideC/side-channel.pdf

9. Bibliography

Side channel attacks:
http://www.cryptofails.com/post/70097430253/crypto-noobs-2-side-channel-attacks

Side-Channel Attacks: Ten Years After Its Publication and the Impacts on Cryptographic Module Security Testing:
http://csrc.nist.gov/groups/STM/cmvp/documents/fips140-3/physec/papers/physecpaper19.pdf

POWER ANALYSIS ON SMARTCARD ALGORITHMS USING SIMULATION:
http://doc.utwente.nl/66569/1/200422.pdf

9. Bibliography

Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?
https://cryptome.org/jya/emr.pdf

TEMPEST: A Signal Problem
https://www.nsa.gov/news-features/declassified-documents/cryptologic-spectrum/assets/files/tempest.pdf

DEF CON 21: Melissa Elliot - Noise Floor
https://youtu.be/CCgSGZ7S-BQ