
# Tempestad en OSX

Pedro C. aka
s4ur0n

incibe_
TRABAJANDO POR LA CONFIANZA DIGITAL

CyberCamp.es

# Whoami


```
class PedroC:
    def __init__(self):
        self.name = 'Pedro Candel'
        self.email1 = 'pcandel@cybersoc.deloitte.es'
        self.email2 = 's4ur0n@s4ur0n.com'
        self.website = 'https://www.s4ur0n.com'
        self.nickname = '@NN2ed_s4ur0n'
        self.role = 'Security Researcher'
        self.interest = [ 'Reversing', 'Malware',
                          'Offensive Security', '…' ]
        self.member_of = [ 'mlw.re', 'OWASP', 'NetXploit', '…' ]
```

Deloitte.
CyberSOC Academy

# Concepts

## Introduction

# Covert Channel

A **covert channel** is a type of computer security attack that creates a capability to transfer information objects between processes that are not supposed to be allowed to communicate by the computer security policy.

The term, originated in 1973 by Lampson, is defined as "*(channels) not intended for information transfer at all, such as the service program's effect on system load*" to distinguish it from ***legitimate*** channels that are subjected to access controls.

Source: https://en.wikipedia.org/wiki/Covert_channel

# Tempest


**TEMPEST** is a National Security Agency specification and **NATO certification** referring to spying on information systems through leaking emanations, including unintentional radio or electrical signals, sounds, and vibrations.

TEMPEST covers ***both methods*** to ***spy upon others*** and ***also how to shield equipment*** against such spying.

The protection efforts are also known as emission security (**EMSEC**), which is a subset of communications security (**COMSEC**).

# Tempest

The **NSA** methods for spying upon computer emissions are classified, but some of the protection standards have been released by either the NSA or the Department of Defense. Protecting equipment from spying is done applying distance, shielding, filtering and masking.

The **TEMPEST standards** mandate elements such as equipment distance from walls, amount of shielding in buildings and equipment, and distance separating wires carrying classified vs. unclassified materials, filters on cables, and even distance and shielding between wires/equipment and building pipes. Noise can also protect information by masking the actual data.

# Tempest


While much of **TEMPEST** is about leaking electromagnetic emanations, ***it also encompasses sounds or mechanical vibrations***. For example, it is possible to log a user's keystrokes using the motion sensor inside smartphones.

Compromising emissions are defined as unintentional intelligence-bearing signals which, if intercepted and analyzed, may disclose the information transmitted, received, handled, or otherwise processed by any information-processing equipment.

Source: https://en.wikipedia.org/wiki/Tempest_(codename)

# Tempest Attacks

Data from electromagnetic waves

# Tempest Attacks


**TEMPEST Attacks** work on the principle that electronic devices such as *monitors* and *fax machines* emit **electromagnetic radiation** during normal use.

With correct equipment such as antennas, receivers and display units an attacker could **in theory** intercept those emissions from a remote location (from across the street perhaps) and then replay the information that was captured.

# Tempest Attacks

**Imagine if this were possib… be misused to viol…**

*Cl… …ng to sto… … disp… exp… …or* ***it's e…*** *…to "capt… …y* ***it's ce…***

# Tempest Attacks


Such an **attack is passive** in that ***it cannot be detected***.

A device emits compromising radiation which **could be reconstructed** from a remote location.

This means that you cannot detect it as the device is not in any way connected/installed on your system.

To simply put it your computer can't detect a guy down the street with equipment trying picking up radio emissions from your monitor.

# Tempest Attacks

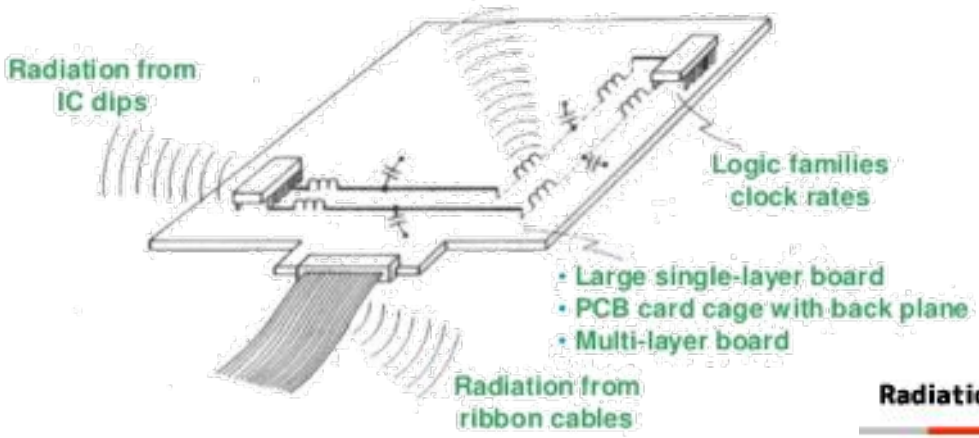

**All electronic devices** big or small ***may emit low-level electromagnetic radiation***.

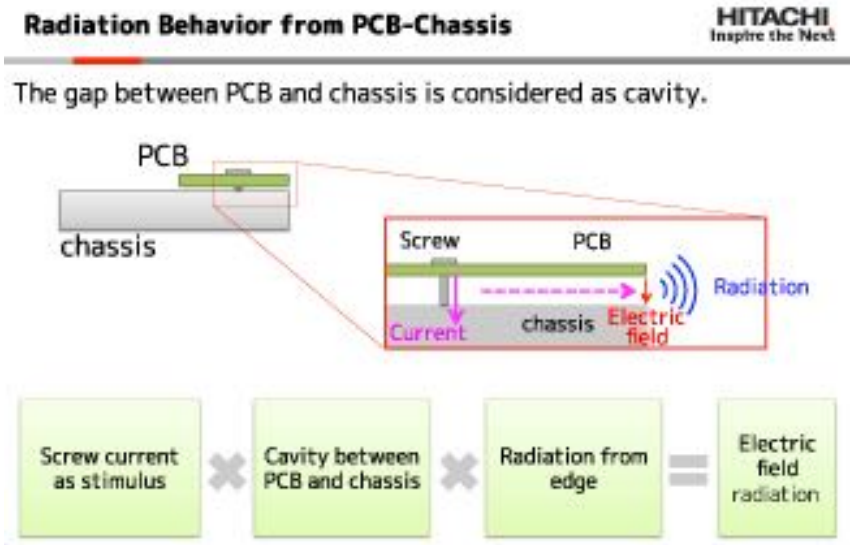
In fact the **CPU chip** is probably doing it right now.

This happens whenever an electric current *changes in voltage* and thus *generates electromagnetic pulses that radiate* as **invisible radio waves**. These electromagnetic radio waves can carry a great distance in ideal situations.

# Tempest Attacks

## PRINCIPAL RADIATION SOURCES ON PRINTED CIRCUIT BOARD



# Tempest Attacks

Is tempest a myth?

# Is tempest a myth or a reality?

If tempe ttackers had a high success rate you wouldn iddle of the night"
break-i

They

All the om a
dista al
data

Really?

# Is tempest a myth or a reality?


Date: Wed, 18 Aug 1999 19:15:09 +0300 (EEST)
From: Berke Durak <durakb@crit2.univ-montp2.fr>
To: cypherpunks@toad.com
Subject: Controlled CPU TEMPEST emanations

Hello,

After having implemented and successfully tested Ross Anderson's idea to use the video output to synthesize a mediumwave AM signal, I wondered if a similar effect could be obtained by using only the CPU, since it was easy to correlate CPU activity with radio noise. I've just written a quick C program that tries to force activity on the memory bus in a repetitive pattern, with adjustable frequency. After having fiddled with the timings for about one hour, I managed to broadcast a test tune using my Pentium 120 running Linux, giving extremely clear reception on FM band at about 87.5 Mhz (I have in no way calculated or predicted this frequency).

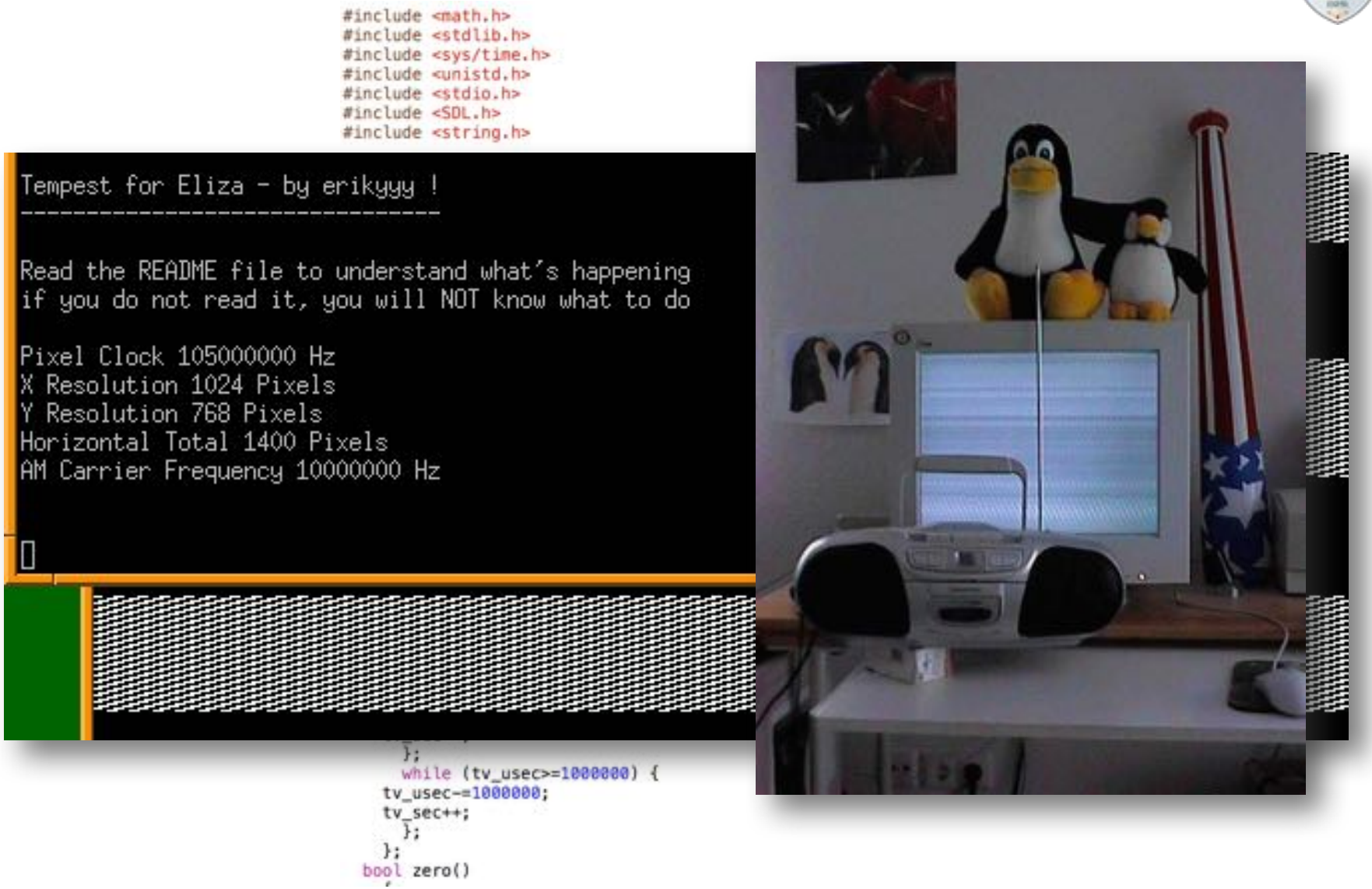
Be warned that my understanding of radio waves is bad and incomplete, and that I have no particular radio equipment, save a walkman and a radio cassette player.

I found that it is possible to hear the test tune over the whole "consumer" medium- and short-wave spectrum (530-1600 KHz, 2.3-22 MHz) using the walkman, which has a digital synthesized PLL radio (which is generally very sensitive to electrical noise), provided the radio is held at a distance of less than two meters around the CPU, which suggests that there are spectral components of CPU activity at many frequencies dividing the clock frequency and at their harmonics (which gives a very rich spectrum). The reception in the FM band is much more clean, and it is possible to hear the test tune in the next room (three to four meters).

I've found that accesses to the main memory create much more noise

Source: https://cryptome.org/tempest-cpu.htm

# Is tempest a myth or a reality?



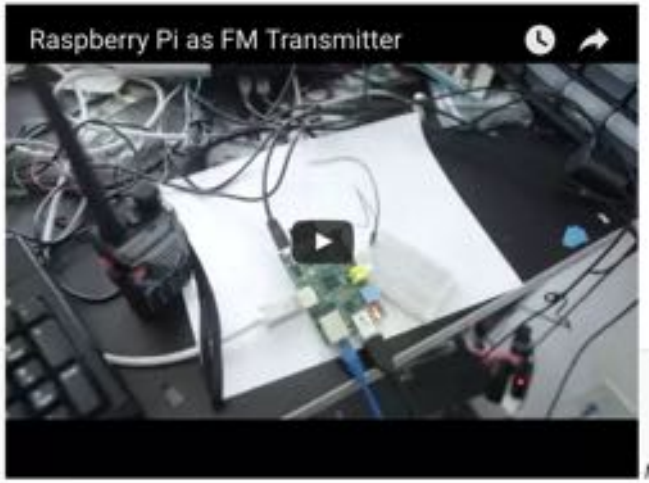

Source: http://www.erikyyy.de/tempest/

# Is tempest a myth or a reality?

## Turning the Raspberry Pi Into an FM Transmitter

**Contents** [hide]






### Steps to play sound:

(Created by Oliver Mattos and Oskar Weigl. Code is GPL)

```
sudo python
>>> import PiFm
>>> PiFm.play_sound("sound.wav")
```

Now connect a 70cm (optimally, ~20cm will do) or so plain wire to GPIO 4 (which is pin 7 on header P1) to act as an antenna, and tune an FM radio to 103.3Mhz.

Download the module here:

- [Download Now!]

(this contains both source and a ready to go binary. Just run the above code in the same folder. The antenna is optional, but range is reduced from ~100 meters to ~10cm without the antenna. Th
format. )

### New! Now with stereo

Source:
http://www.icrobotics.co.uk/wiki/index.php/Turning_the_Raspberry_Pi_Into_an_FM_Transmitter

# Is tempest a myth or a reality?

Cornell University
Cornell University Library

arXiv.org > cs > arXiv:1606.05915

Search or Article ID inside arXiv | All papers | Broaden yo

(Help | Advanced search)

Computer Science > Cryptography and Security

## Fansmitter: Acoustic Data Exfiltration from (Speakerless) Air-Gapped Computers

Mordechai Guri, Yosef Solewicz, Andrey Daidakulov, Yuval Elovici

(Submitted on 19 Jun 2016)

Because computers may contain or interact with sensitive information, they are often air-gapped and in this way kept isolated and disconnected from the Internet. In recent years the ability of malware to communicate over an air-gap by transmitting sonic and ultrasonic signals from a computer speaker to a nearby receiver has been shown. In order to eliminate such acoustic channels, current best practice recommends the elimination of speakers (internal or external) in secure computers, thereby creating a so-called 'audio-gap'. In this paper, we present Fansmitter, a malware that can acoustically exfiltrate data from air-gapped computers, even when audio hardware and speakers are not present. Our method utilizes the noise emitted from the CPU and chassis fans which are present in virtually every computer today. We show that a software can regulate the internal fans' speed in order to control the acoustic waveform emitted from a computer. Binary data can be modulated and transmitted over these audio signals to a remote microphone (e.g., on a nearby mobile phone). We present Fansmitter's design considerations, including acoustic signature analysis, data modulation, and data transmission. We also evaluate the acoustic channel, present our results, and discuss countermeasures. Using our method we successfully transmitted data from air-gapped computer without audio hardware, to a smartphone receiver in the same room. We demonstrated the effective transmission of encryption keys and passwords from a distance of zero to eight meters, with bit rate of up to 900 bits/hour. We show that our method can also be used to leak data from different types of IT equipment, embedded systems, and IoT devices that have no audio hardware, but contain fans of various types and sizes.

Subjects: Cryptography and Security (cs.CR)
Cite as: arXiv:1606.05915 [cs.CR]
(or arXiv:1606.05915v1 [cs.CR] for this version)

**Submission history**

From: Mordechai Guri [view email]
[v1] Sun, 19 Jun 2016 22:05:44 GMT (2125kb)

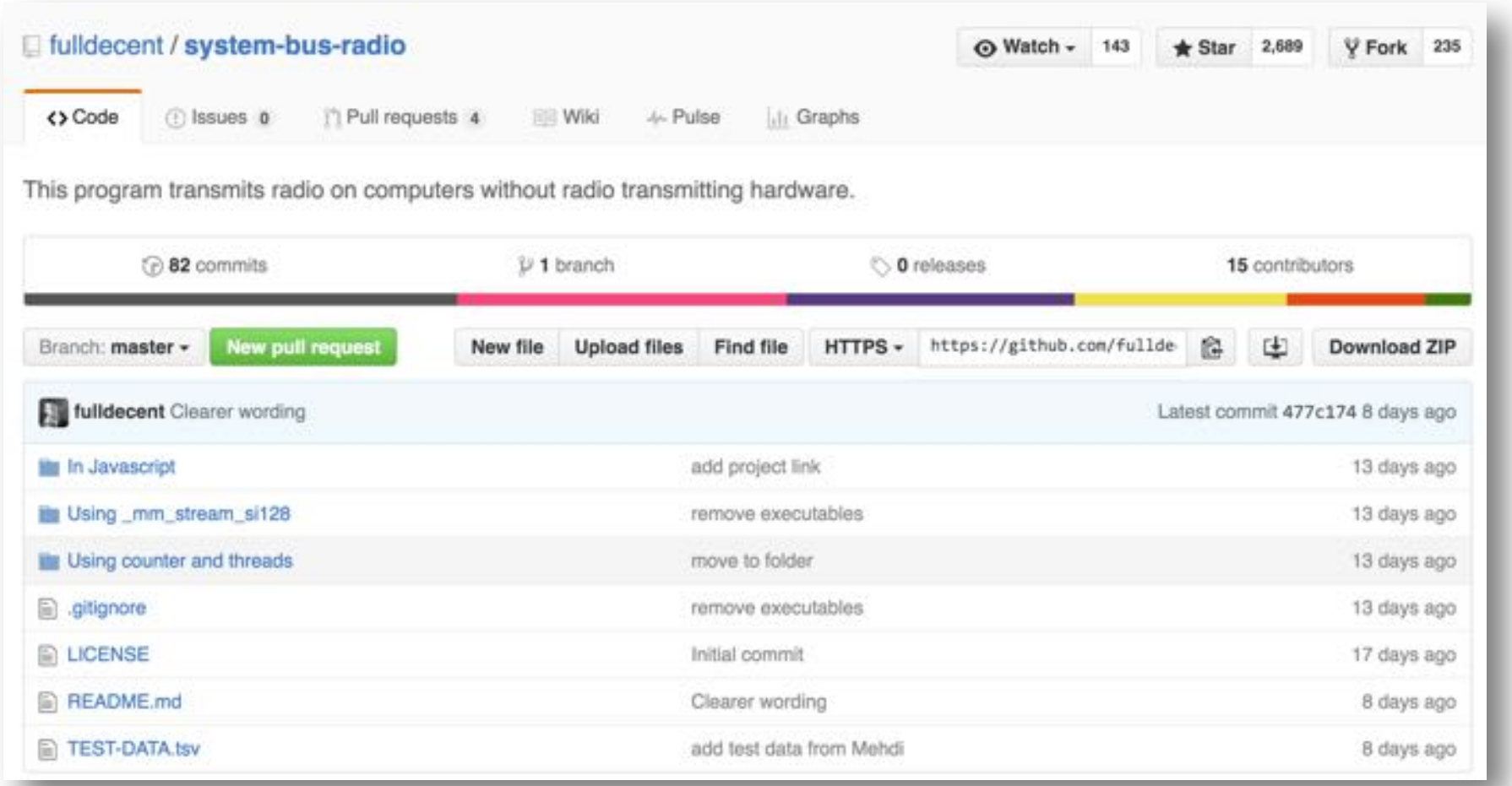
Source(s): https://arxiv.org/abs/1608.03431 &
https://arxiv.org/abs/1606.05915

# Tempest OSX

## New covert channel

# Tempest OSX

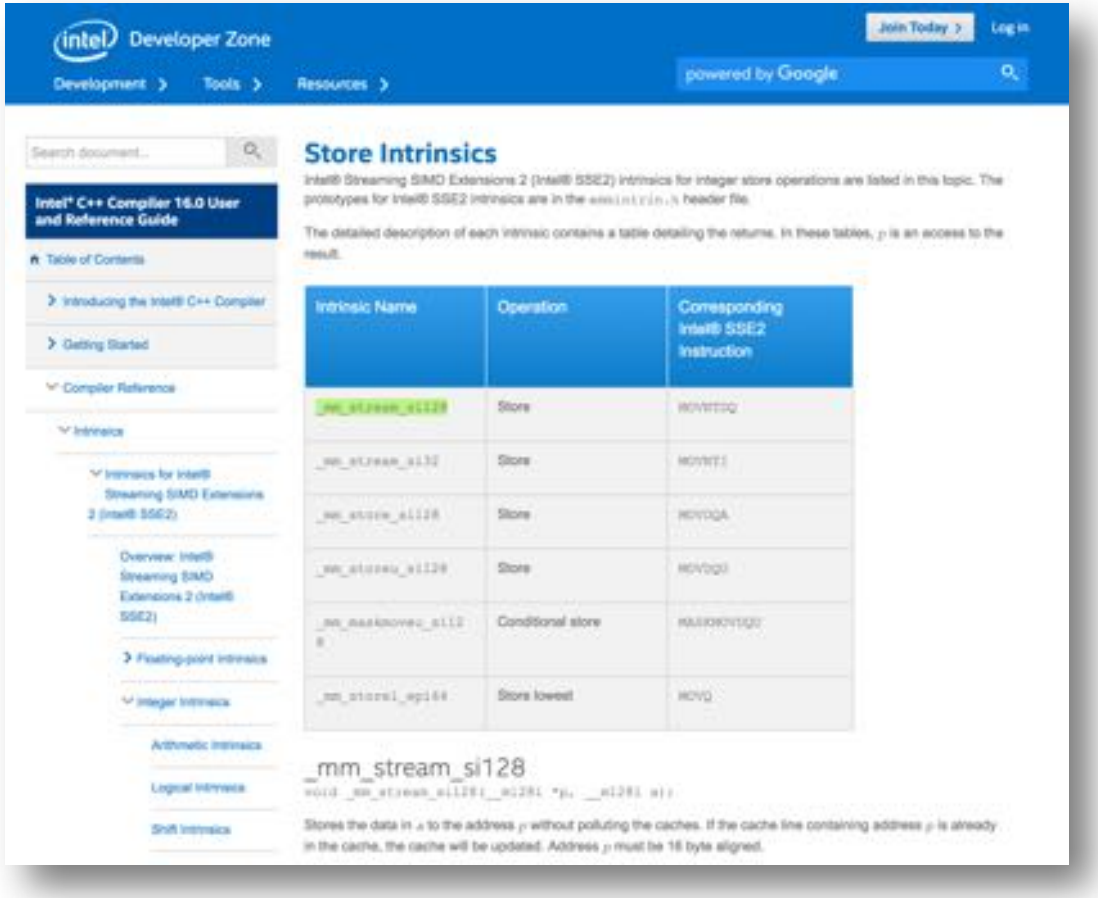
## System Bus Radio: the start point




Source: https://github.com/fulldecent/system-bus-radio

# Tempest OSX

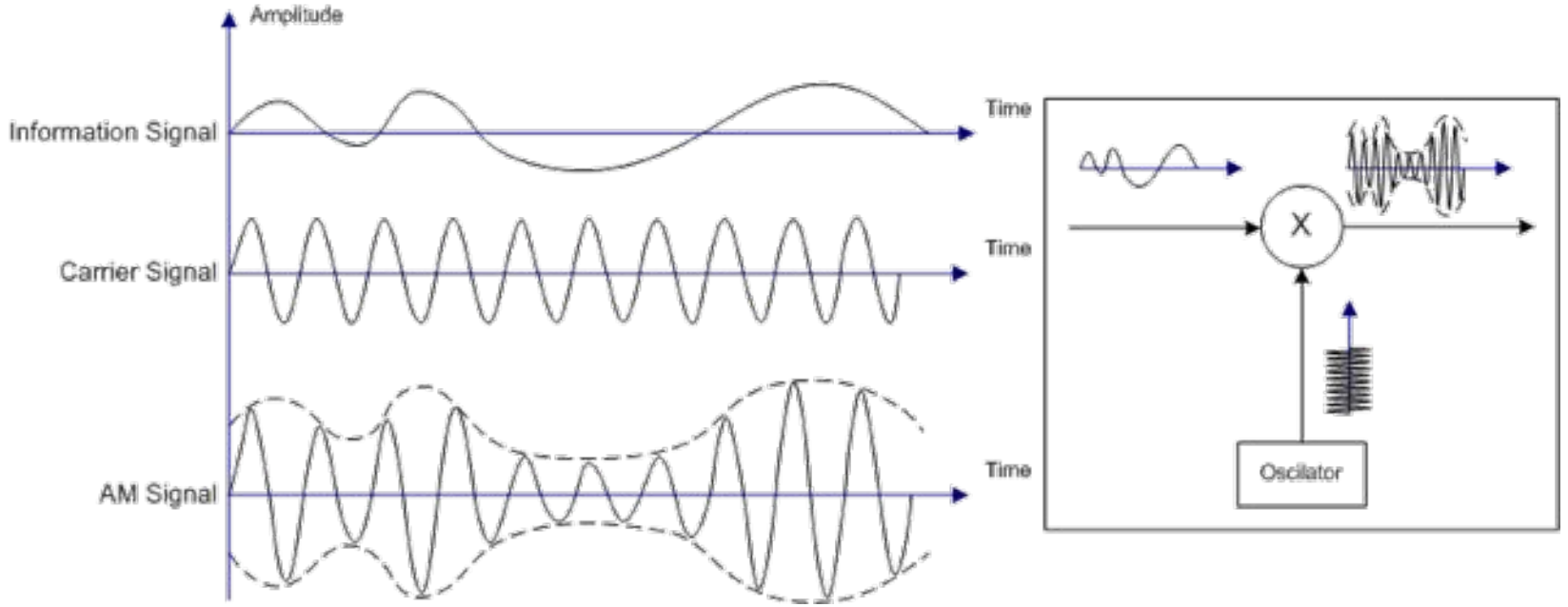
**How to**: Run instructions on the computer that **cause electromagnetic radiation** (*taking advantage of the noise generated*)



# Tempest OSX

**How to**: transmit information via a radio carrier wave

In **amplitude modulation**, the *amplitude* (signal strength) of the carrier wave is varied in proportion to the waveform being transmitted.



# Tempest OSX

The actual emissions are caused by the `_mm_stream_si128` instruction that writes through to a memory address. Inspiration for using this instruction was provided in:

> Guri, M., Kachlon, A., Hasson, O., Kedma, G., Mirsky, Y. and Elovici, Y., 2015. GSMem: data exfiltration from air-gapped computers over GSM frequencies. In 24th USENIX Security Symposium (USENIX Security 15) (pp. 849-864).

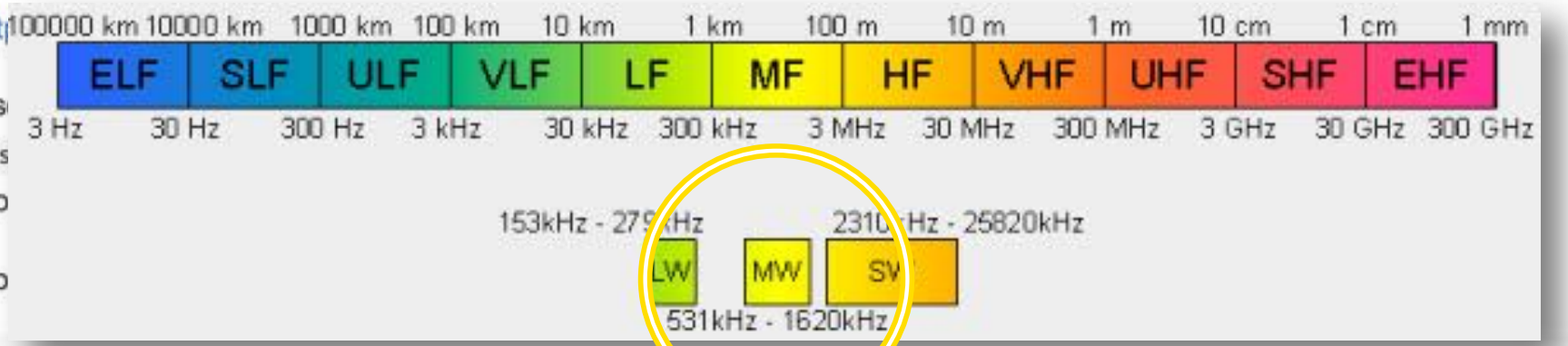
htt

Pleas

_mm_s

impro

The p




```
|<--------------------TIME--------------------->|
|                                               |
|¯|_|¯|_|¯|_____________|¯|_|¯|_|¯|_____________
|                       |   |   |
|<------SIGNAL--------->|   |   |
                        |   |
                        |<->| CARRIER
```

# Tempest OSX

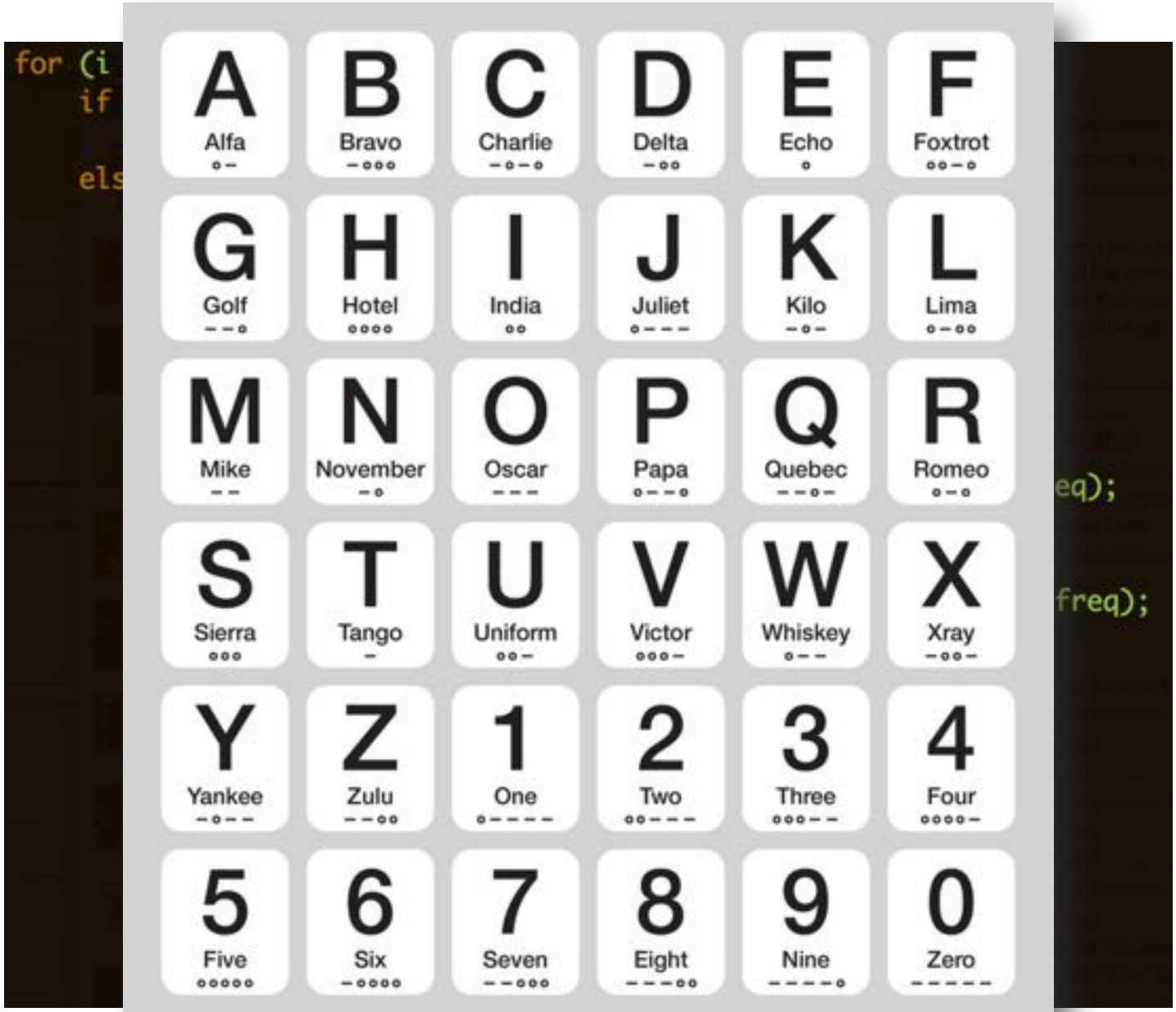

```
#define basefreq 880.00 // C7 (http://hyperphysics.phy-astr.gsu.edu/hbasees/music/imgmus/etfreq.gif)
#define notaudible 0
```

```
static inline void square_am_signal(float time, float frequency) {
  printf("Playing / %0.3f seconds / %4.0f Hz\n", time, frequency);
        uint64_t period = NSEC_PER_SEC / frequency;

        uint64_t start = mach_absolute_time();
        uint64_t end = start + time * NSEC_PER_SEC;

        while (mach_absolute_time() < end) {
    uint64_t mid = start + period / 2;
                uint64_t reset = start + period;
    while (mach_absolute_time() < mid) {
      _mm_stream_si128(&reg, reg_one);
      _mm_stream_si128(&reg, reg_zero);
    }
    clock_sleep_trap(clock_port, TIME_ABSOLUTE, reset / NSEC_PER_SEC, reset % NSEC_PER_SEC, &remain);
                start = reset;
        }
}
```

# Tempest OSX


A Alfa
B Bravo
C Charlie
D Delta
E Echo
F Foxtrot
G Golf
H Hotel
I India
J Juliet
K Kilo
L Lima
M Mike
N November
O Oscar
P Papa
Q Quebec
R Romeo
S Sierra
T Tango
U Uniform
V Victor
W Whiskey
X Xray
Y Yankee
Z Zulu
1 One
2 Two
3 Three
4 Four
5 Five
6 Six
7 Seven
8 Eight
9 Nine
0 Zero

# Demo

# Tempest OSX

If we can find no answer
to these problems, then
we really are in trouble

# Tempest OSX


**Houston, we have a problem**

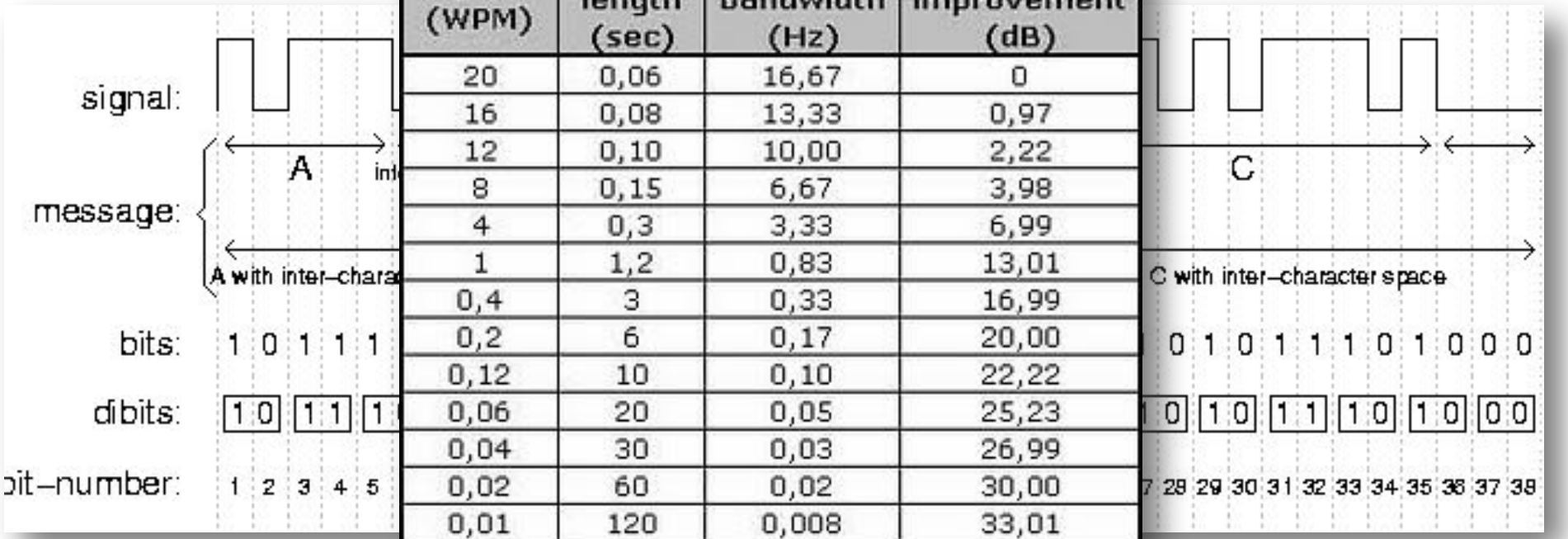
Broadcast transmission ☹

You need the receiving person or machine to be able to understand morse code ☹

Binary files ☹

Limited set of characters ☹

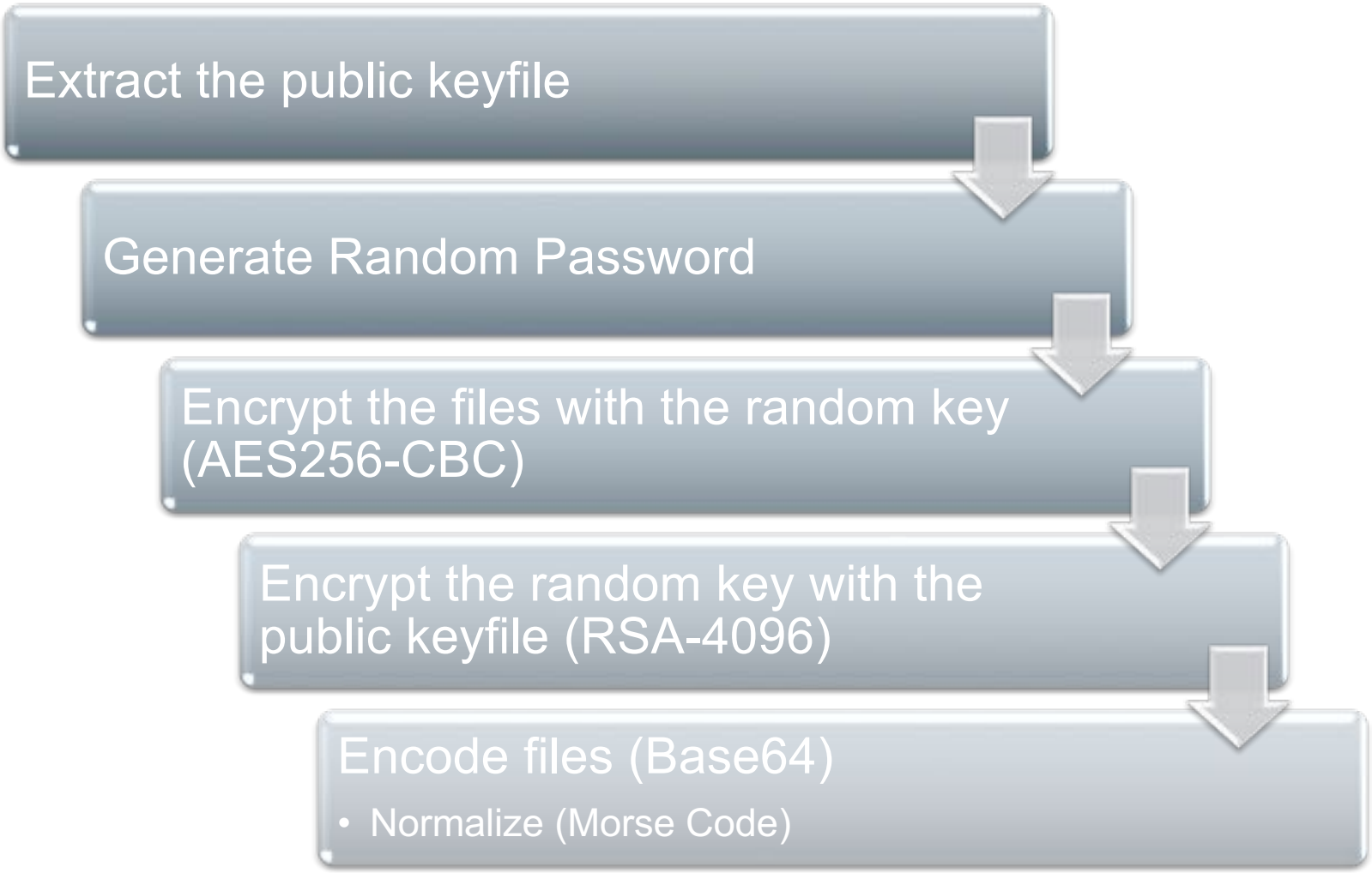
# Variable Speed (WPM)




| Speed (WPM) | Dot length (sec) | Optimum bandwidth (Hz) | SNR improvement (dB) |
|---|---|---|---|
| 20 | 0,06 | 16,67 | 0 |
| 16 | 0,08 | 13,33 | 0,97 |
| 12 | 0,10 | 10,00 | 2,22 |
| 8 | 0,15 | 6,67 | 3,98 |
| 4 | 0,3 | 3,33 | 6,99 |
| 1 | 1,2 | 0,83 | 13,01 |
| 0,4 | 3 | 0,33 | 16,99 |
| 0,2 | 6 | 0,17 | 20,00 |
| 0,12 | 10 | 0,10 | 22,22 |
| 0,06 | 20 | 0,05 | 25,23 |
| 0,04 | 30 | 0,03 | 26,99 |
| 0,02 | 60 | 0,02 | 30,00 |
| 0,01 | 120 | 0,008 | 33,01 |
| 0,004 | 300 | 0,003 | 36,99 |
| 0,002 | 600 | 0,002 | 40,00 |

# Tempest OSX

## Encode & cipher



# Tempest OSX

## Encode (Base64)

| Value | Char | Value | Char | Value | Char | Value | Char |
|---|---|---|---|---|---|---|---|
| 0 | A | 16 | Q | 32 | g | 48 | w |
| 1 | B | 17 | R | 33 | h | 49 | x |
| 2 | C | 18 | S | 34 | i | 50 | y |
| 3 | D | 19 | T | 35 | j | 51 | z |
| 4 | E | 20 | U | 36 | k | 52 | 0 |
| 5 | F | 21 | V | 37 | l | 53 | 1 |
| 6 | G | 22 | W | 38 | m | 54 | 2 |
| 7 | H | 23 | X | 39 | n | 55 | 3 |
| 8 | I | 24 | Y | 40 | o | 56 | 4 |
| 9 | J | 25 | Z | 41 | p | 57 | 5 |
| 10 | K | 26 | a | 42 | q | 58 | 6 |
| 11 | L | 27 | b | 43 | r | 59 | 7 |
| 12 | M | 28 | c | 44 | s | 60 | 8 |
| 13 | N | 29 | d | 45 | t | 61 | 9 |
| 14 | O | 30 | e | 46 | u | 62 | + |
| 15 | P | 31 | f | 47 | v | 63 | / |

# Tempest OSX

**Enc**

Inte

## The International Morse Code

A dash is equal to three dots in time, while the interval between the dots and dashes in a letter equals a dot in time. Between the letters in a word the interval is equal to three dots and between words, five dots.

### THE ALPHABET

| | | | |
|---|---|---|---|
| A | ·— | N | —· |
| B | —··· | O | ——— |
| C | —·—· | P | ·——· |
| D | —·· | Q | ——·— |
| E | · | R | ·—· |
| F | ··—· | S | ··· |
| G | ——· | T | — |
| H | ···· | U | ··— |
| I | ·· | V | ···— |
| J | ·——— | W | ·—— |
| K | —·— | X | —··— |
| L | ·—·· | Y | —·—— |
| M | —— | Z | ——·· |

### ACCENTED LETTERS

| | |
|---|---|
| Ā | ·—·— |
| À or Å | ·——·— |
| CH | ———— |
| É | ··—·· |
| Ñ | ——·—— |
| Ö | ———· |
| Ü | ··—— |

### NUMERALS

| | | | |
|---|---|---|---|
| 1 | ·———— | 6 | —···· |
| 2 | ··——— | 7 | ——··· |
| 3 | ···—— | 8 | ———·· |
| 4 | ····— | 9 | ————· |
| 5 | ····· | 0 | ————— |

### ABBREVIATED NUMERALS

| | | | |
|---|---|---|---|
| 1 | ·— | 6 | —···· |
| 2 | ··— | 7 | ——··· |
| 3 | ···— | 8 | ———·· |
| 4 | ····— | 9 | ————· |
| 5 | ····· (or ·) | 0 | ————— |

### PUNCTUATION AND OTHER SIGNS

| | |
|---|---|
| Full Stop (.) | ·—·—·— |
| Comma (,) | ——··—— |
| Colon (:) | ———··· |
| Hyphen or Dash (-) | —····— |
| Apostrophe (') | ·————·— |
| Fraction Bar (/) | —··—· |
| Separation Sign (between whole number and fraction) | ·—·—· |
| *Brackets [( )] | —·——·—— |
| *Underline | ··——·— |
| Break or Double Dash (=) | —···— |
| Interrogation Mark (?) | ··——··— |
| Erase (or Error) | ·········· |
| Starting Signal | —·—·— |
| End of Message | ·—·—· |
| Closing Down | ···——·— |
| Interval (Wait) | ·———··· |
| Message Received | ·—·· |
| Ready to Receive | —·— |
| Distress Call or SOS | ···———··· |

* The " brackets " and " underline " signs are transmitted before and after the word or words affected.

# Tempest OSX


## Normalize

Substitutions:

| Change | Substitution | Morse Code |
|---|---|---|
| Upper to lower | Insert Colon : & Uppercase(char) | - - - . . . + toupper(char) |
| Plus (+) | Minus (-) | - . . . . - |
| Interfile Space | Apostrophe (´) | . - - - - . |

# Demo

# Tempest OSX

## Next steps

- Select
- SDR c … up
- Direct
- Low p
- Radio
- Encoc … A (ASCII),
- …
- BadU
- …

CONFIRMED!

# Questions?


cyber
camp
CYBERSECURITY EVENT
2015
Gracias por
su atención
GOBIERNO
DE ESPAÑA
MINISTERIO
DE ENERGÍA, TURISMO
Y AGENDA DIGITAL
incibe_
TRABAJANDO POR
LA CONFIANZA DIGITAL