Ham crypto

La cryptographie au service des radioamateurs

Quentin F4IRO

Objectifs

- explorer
- théoriser
- discuter

Scénario

Contrôle par service amateur de

- station de base
- relai
- satellite
- …

Plan

1. Cryptographie (9 slides)
2. Réglementation (5 slides)
3. Application (4 slides)

1. Cryptographie

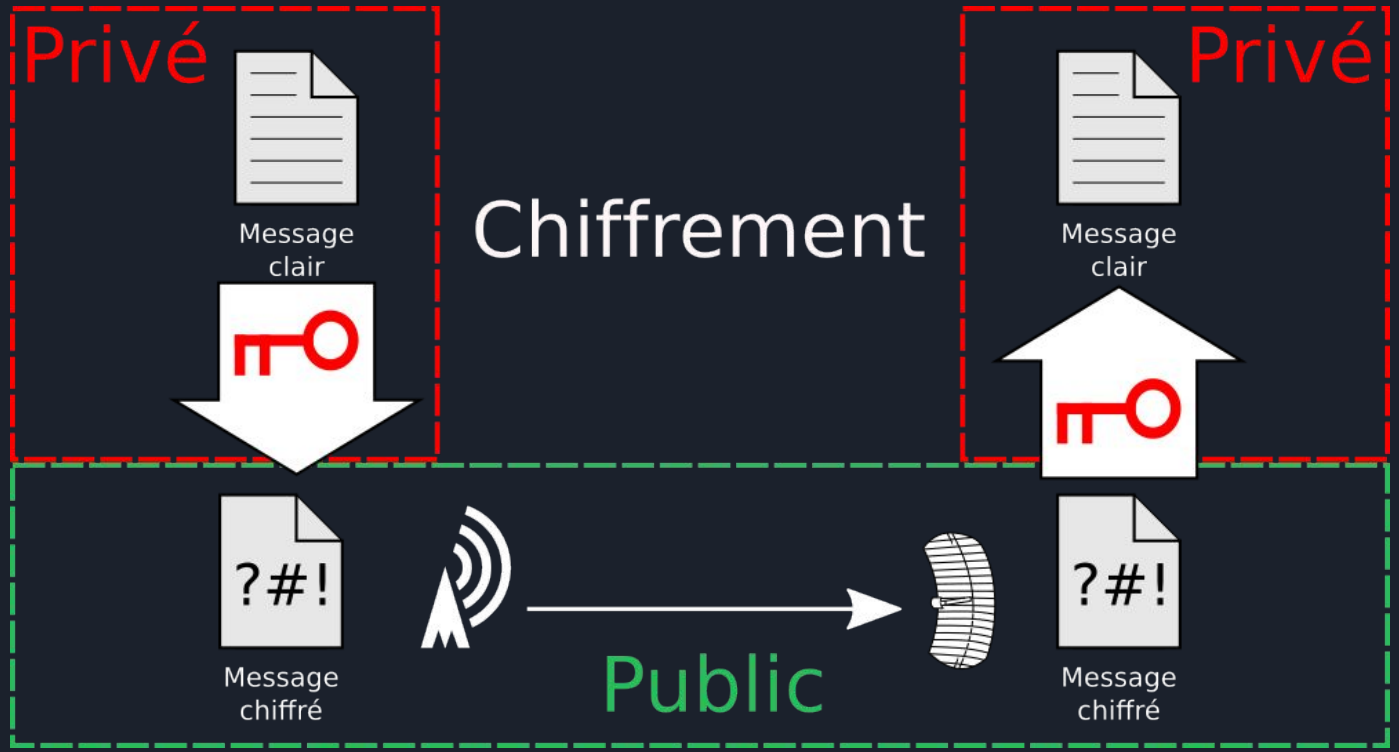
Cryptographie

Communiquer de manière sûre en la présence d'un adversaire

- confidentialité (par ex. IND-CCA)
- authentification (par ex. EUF-CMA)

Chiffrement

Chiffrement : principe

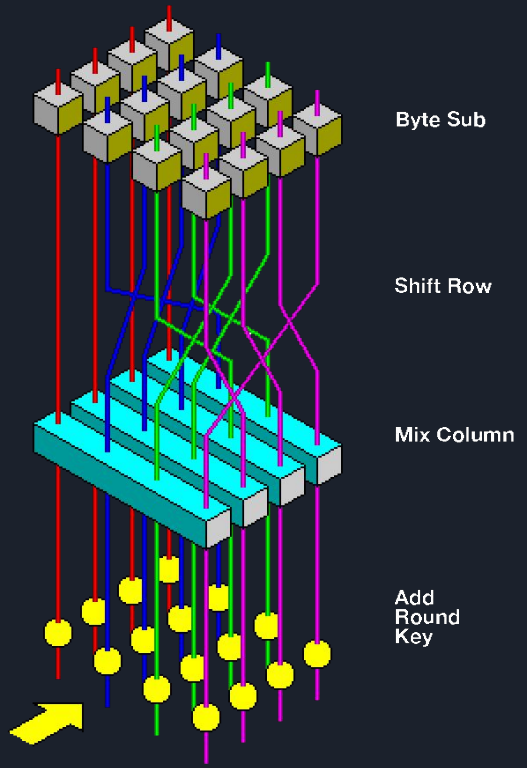


Chiffrement : exemple

Chiffre de César

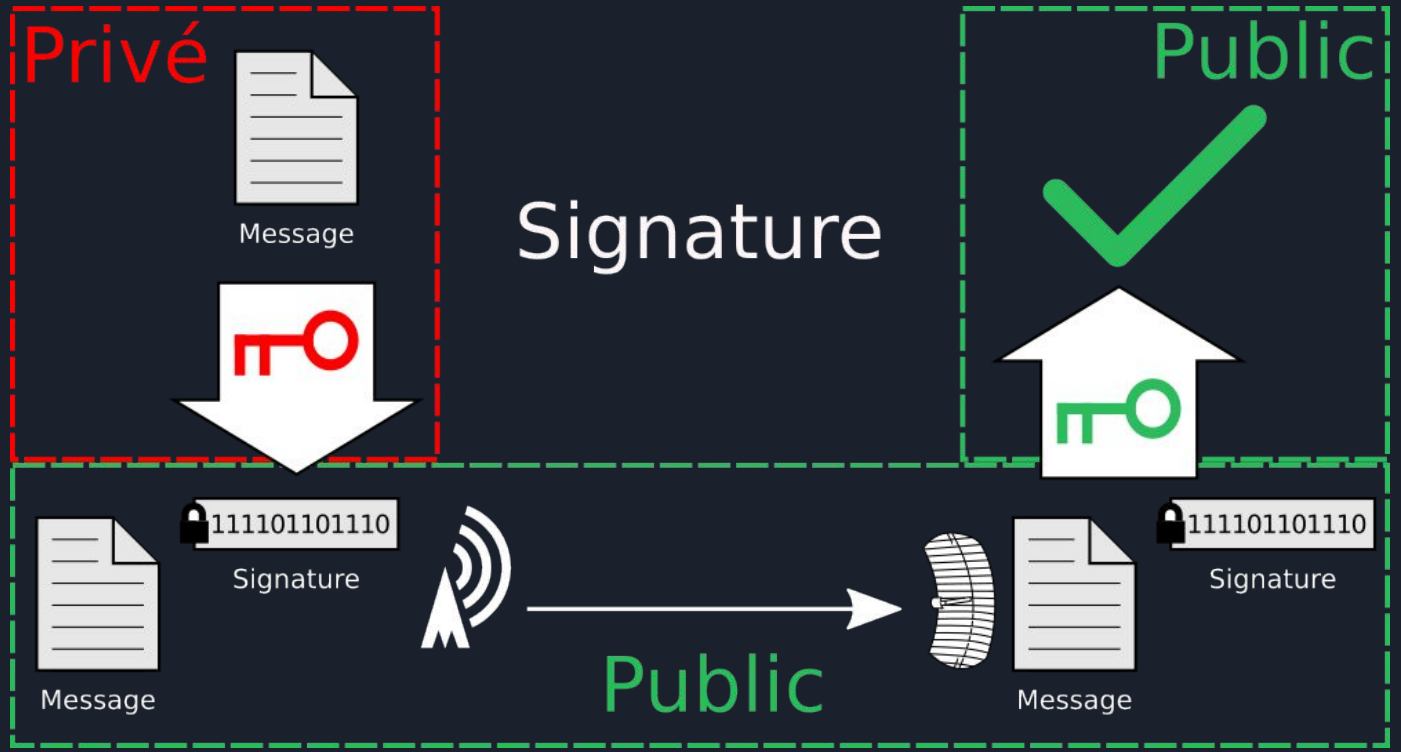
Chiffrement : dans la vraie vie

- *DES (1977)*
- AES (1998)
- Chacha20 (2008)



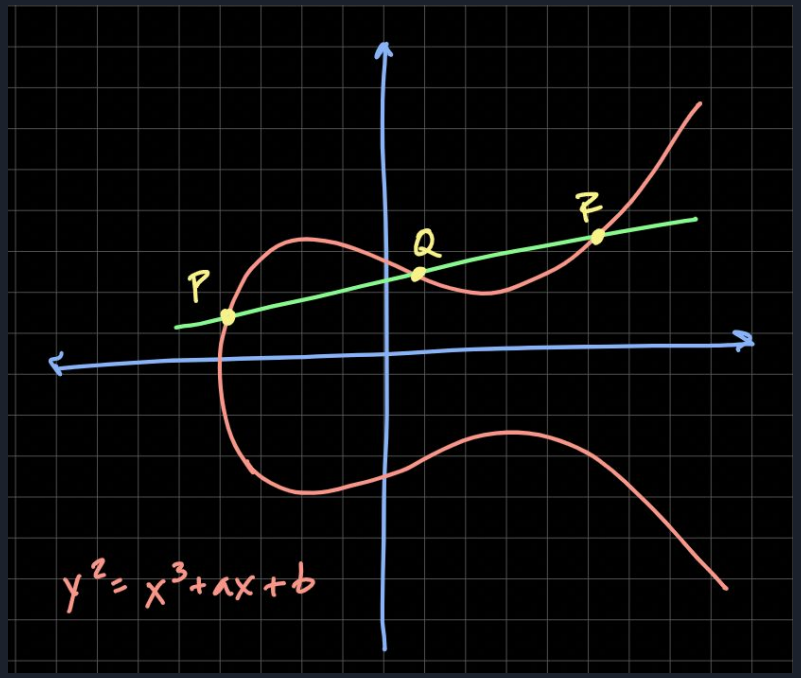
Signature

Signature : principe



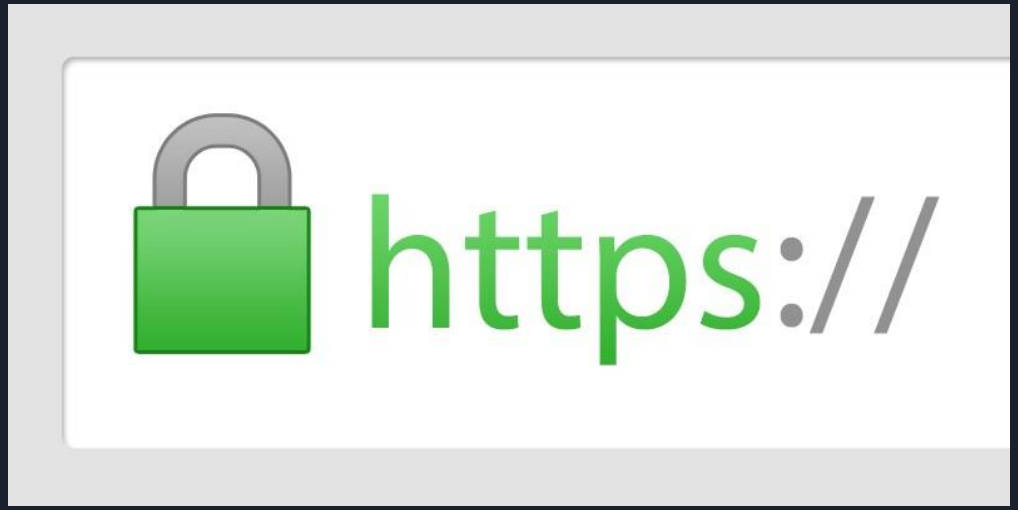
Signature : dans la vraie vie

- RSA (1977)
- DSA (1994)
- ECDSA (1999)

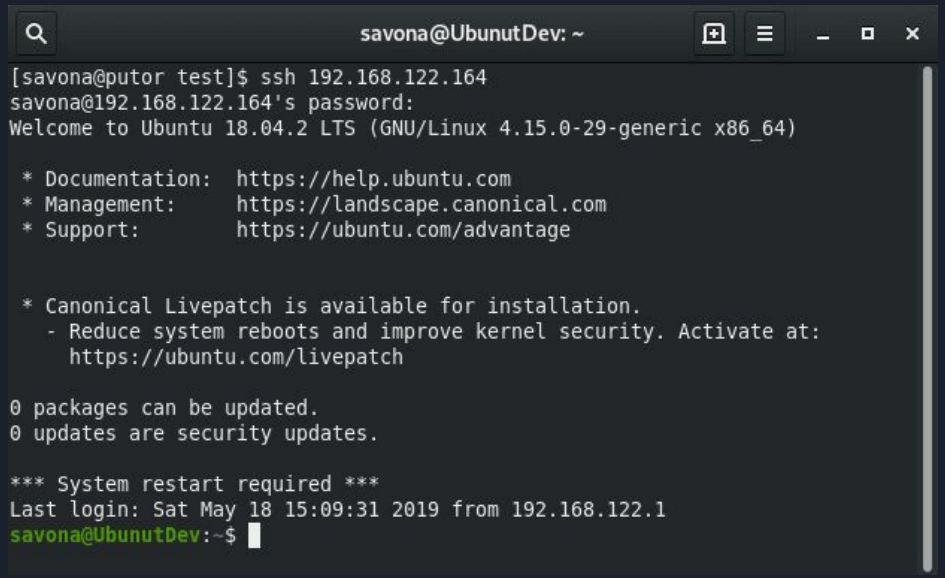


En pratique

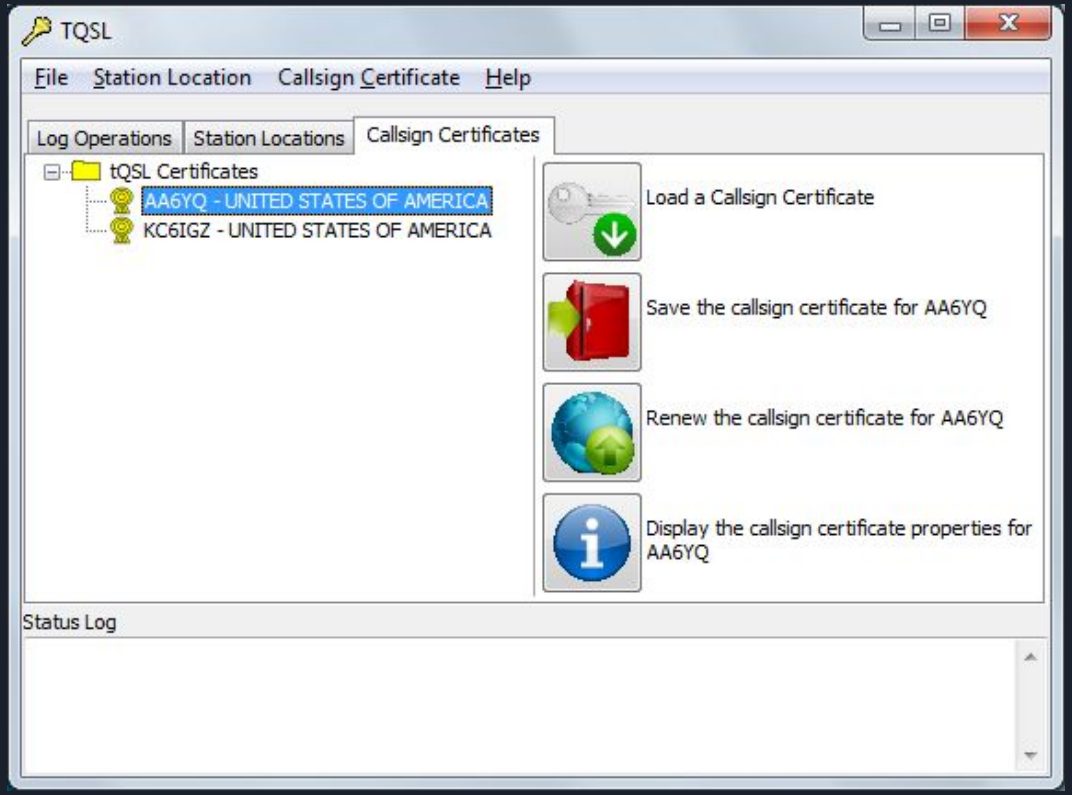
En pratique : HTTPS



En pratique : SSH



En pratique : TQSL



2. Réglementation

Réglementation

Décision № 2012-1241 Article 1

« Il est interdit de coder les transmissions entre des stations d'amateur **pour en obscurcir le sens** »

Réglementation

Chiffrement

(sauf 🛰️)

Réglementation

Signature

Réglementation

Authentification sans chiffrement ?

Réglementation : une idée originale ?

- 1986 https://www.tapr.org/pdf/CNC1986-AuthenticationOfSwitchControlLink-WB3KDU.pdf
- 1991 https://cdn.preterhuman.net/texts/cryptography/arrl.txt
- 2004 https://rietta.com/blog/authentication-without-encryption-for/
- 2010 https://tapr.org/wp-content/uploads/DCC2010-AX.25-AuthenticationEffects-KE5LKY.pdf
- 2013 https://link.springer.com/chapter/10.1007/978-3-642-36169-2_1 ou https://sci-hubtw.hkvisa.net/10.1007/978-3-642-36169-2_1
- 2014 https://rsaxvc.net/blog/2014/2/1/Encryption_and_Amateur_Radio.html
- 2014 https://www.metzdowd.com/pipermail/cryptography/2014-March/020598.html
- 2014 https://old.reddit.com/r/amateurradio/comments/2ct984/is_there_any_legal_way_to_use_encryptioncyphers/
- 2015 https://www.ka2ddo.org/ka2ddo/ARETF-APRS-Authentication.txt
- 2016 https://www.cix.co.uk/~klockstone/201605_Authentication.pdf
- 2016 https://old.reddit.com/r/amateurradio/comments/4nbxrq/authentication_schemes_in_amateur_radio/
- 2016 https://hamwan.org/Administrative/Internet%20and%20Part%2097.html
- 2018 https://github.com/brannondorsey/chattervox
- 2019 https://ham.stackexchange.com/a/12995
- 2019 https://news.ycombinator.com/item?id=19482786
- 2019 https://perens.com/2019/07/02/yes-it-is-legal-to-use-cryptographic-signature-on-amateur-radio-and-thats-important/
- 2020 https://crypto.stackexchange.com/questions/80717/16-bit-2-byte-digital-signature
- 2020 https://hackaday.com/2020/11/28/ham-radio-needs-to-embrace-the-hacker-community-now-more-than-ever/
- 2021 https://old.reddit.com/r/amateurradio/comments/ogrxko/encryption_is_forbidden_but_what_about/
- 2022 https://github.com/aredn/aredn/issues/344
- 2022 https://ham.stackexchange.com/questions/20984/digital-protocols-public-documentation-and-encoded-messages
- 2022 https://hackaday.com/2022/07/15/helping-secure-amateur-radios-digital-future/
- 2022 https://old.reddit.com/r/amateurradio/comments/w8w5wf/does_sending_encrypted_files_over_nonencrypted/ihrt9uo/
- 2022 https://archive.org/details/youtube-FfQpH3PvjDU

3. Application

HTTPS over Ham

Quel navigateur Web ?

SSH over Ham

```
~  echo ' Lorem ipsum dolor sit amet, consectetur adipiscing elit. Curabitur la
cinia tortor ipsum, et suscipit mi mattis eget. Duis vehicula neque quis risus
gravida, sit amet gravida dui rhoncus. Sed sit amet sapien eu risus porttitor e
leifend sit amet vel eros. Morbi interdum venenatis nisi, id scelerisque velit
pharetra accumsan. Nullam vehicula turpis vitae sapien iaculis, ut suscipit qua
m viverra. Vestibulum mattis vehicula volutpat. Cras turpis sem, feugiat at fin
ibus sit amet, vehicula non justo.'
```

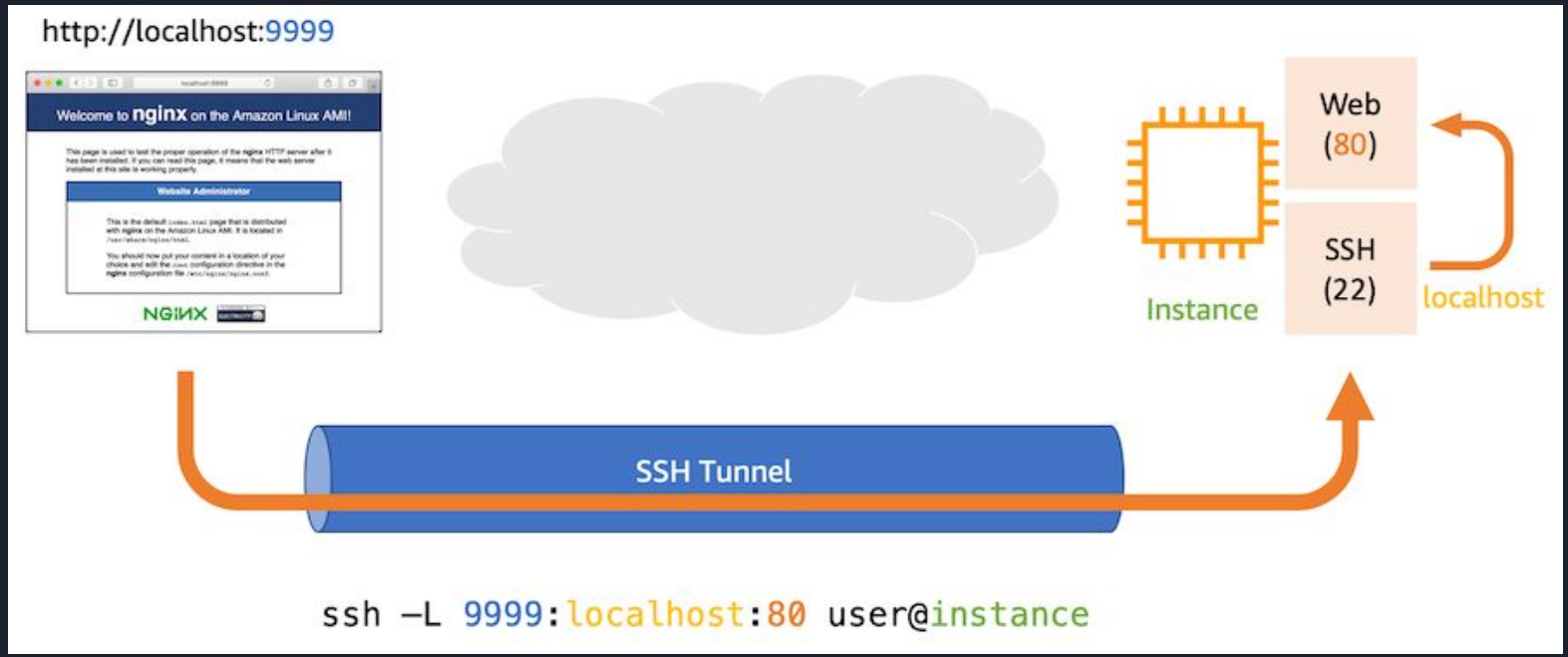
Wireshark · Suivre le flux TCP (tcp.stream eq 0) · Loopback: lo

```
.....^........
..........XN......^.........[?1l.>........r.....<... .^.........[?2004l

............]..@.......        ^........ Lorem ipsum dolor sit amet,
consectetur adipiscing elit. Curabitur lacinia tortor ipsum, et suscipit mi
mattis eget. Duis vehicula neque quis risus gravida, sit amet gravida dui
rhoncus. Sed sit amet sapien eu risus porttitor eleifend sit amet vel eros.
Morbi interdum venenatis nisi, id scelerisque velit pharetra accumsan. Nullam
vehicula turpis vitae sapien iaculis, ut suscipit quam viverra. Vestibulum
mattis vehicula volutpat. Cras turpis sem, feugiat at finibus sit amet,
vehicula non justo.
.........k...
Z.....x.^.......g.[1m.[7m%.[27m.[1m.[0m

...................8.^.......'
.[0m.[27m.[24m.[J.[32m~.[30m%.[37m .[K.......?.....^.........[?
1h.=........I.F.........^.........[?2004h......A.?.82&E
```

HTTP over SSH over Ham



Prochaines étapes

- activer le NULL cipher dans Firefox ?
- comment distribuer ? F6KGL OS ?
- que contrôler ? Raspberry Pi ?