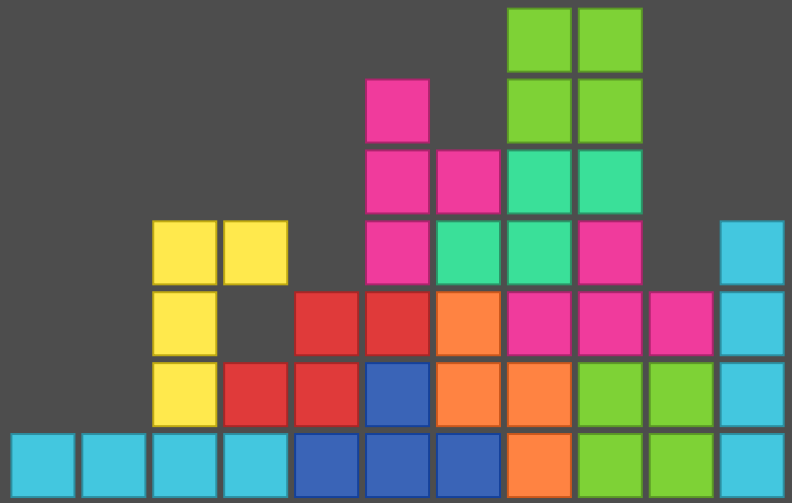
Samba in love with GnuTLS

SambaXP 2019

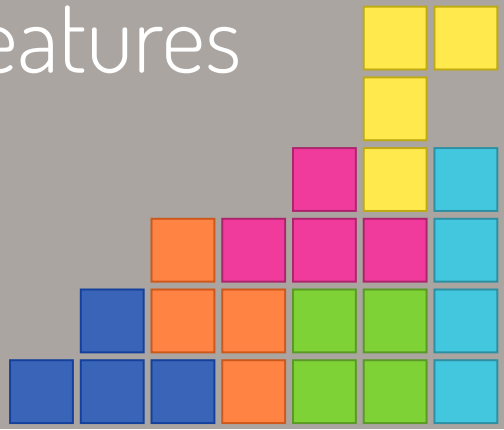
Andreas Schneider
Red Hat Samba Maintainer

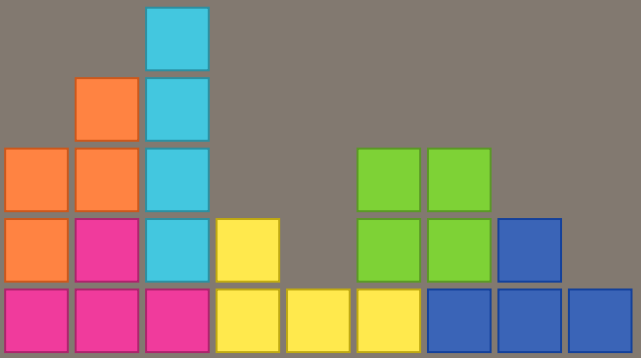


About me

Free and Open Source Software Developer

- cmocka - a unit testing framework for C
- Samba - The domain controller and file server
- libssh - The SSH Library
- cwrap - Client/Server testing made easy
- LineageOS - Android with Privacy Features



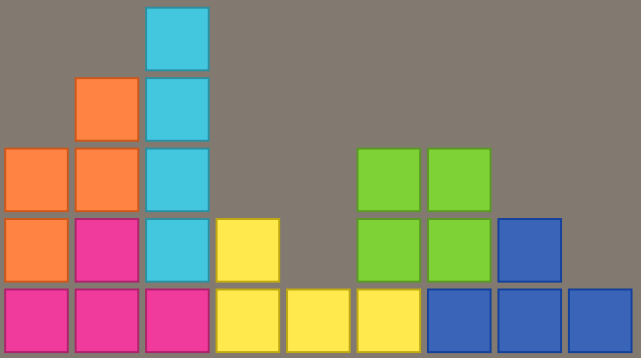


1

What is Samba?

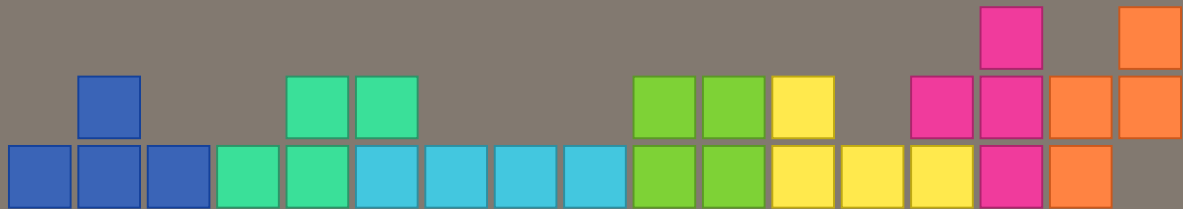
What is Samba?

Samba is the software that you probably curse a lot at.



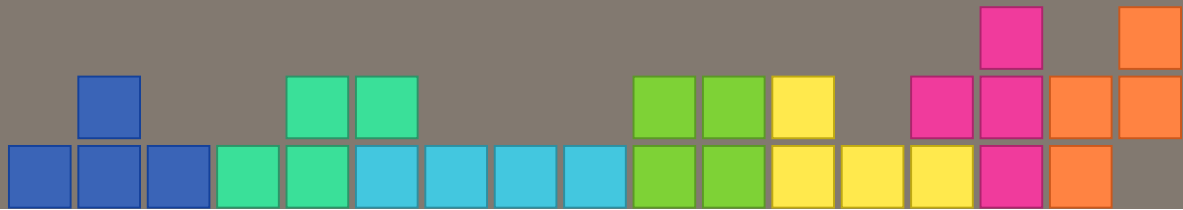
2

What is GnuTLS?



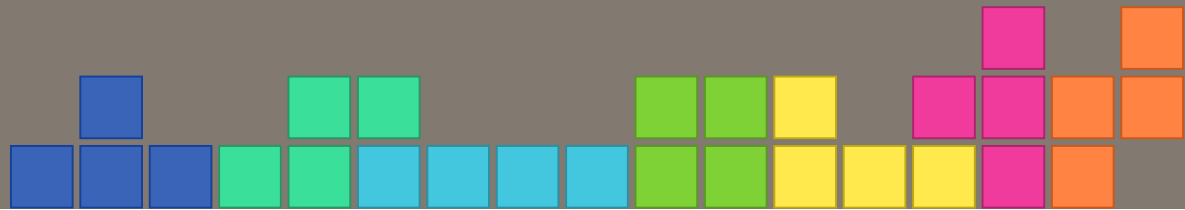
What is GnuTLS?

GnuTLS is the software you will love after this talk.



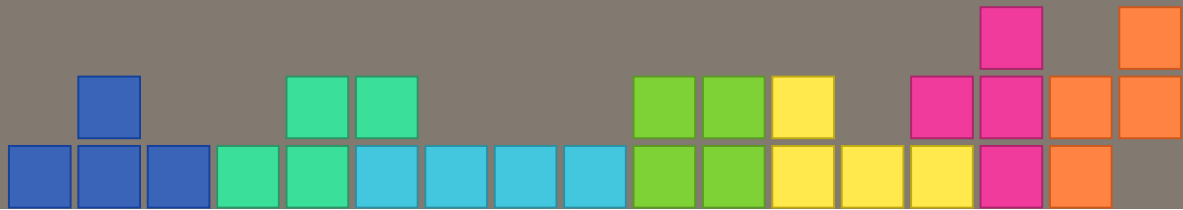
GnuTLS is ...

- Secure communication library for C
- Implements TLS protocol and sourrounding technology
- Mostly uses the nettle library for low level crypto
- Provides more hardware-accelerated implementation of different ciphers



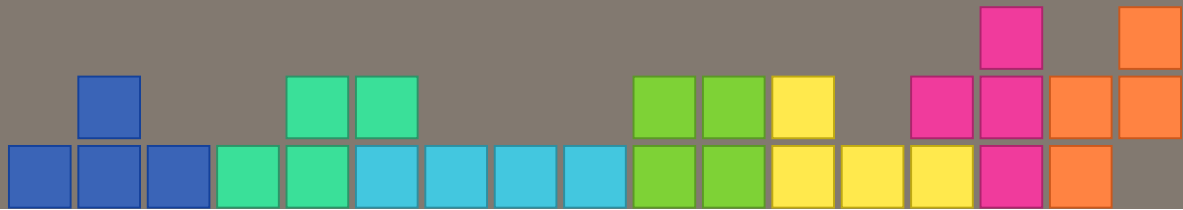
3

Why GnuTLS?



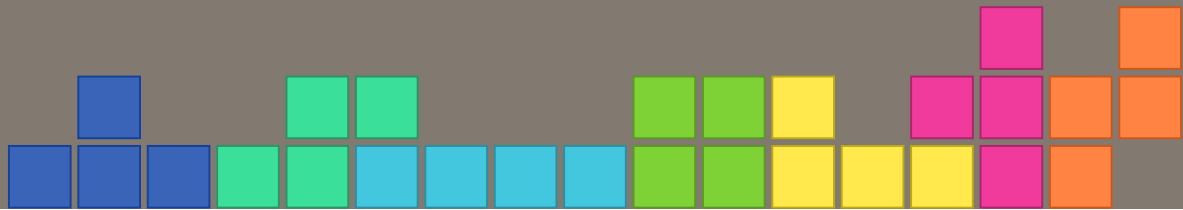
Why do we use GnuTLS?

Samba already uses GnuTLS for LDAP over TLS.



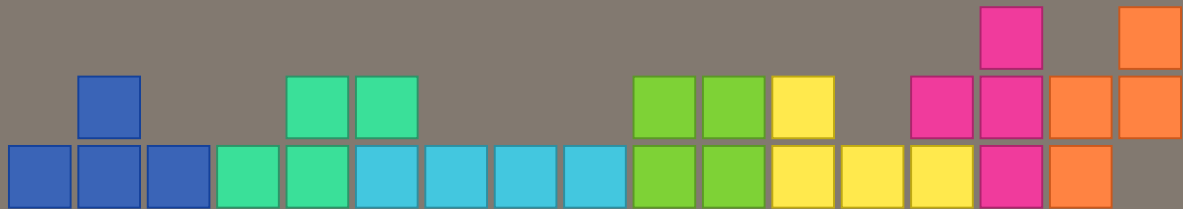
Samba crypto

- Samba implemented own crypto:
  - SHA265, SHA512, HMAC-SHA256
  - MD5, MD4, HMAC-MD5
  - AES-CFB, AES-CCM, AES-GCM, AES-CMAC
  - DES, RC4



4

Why shouldn't you write your own crypto functions?

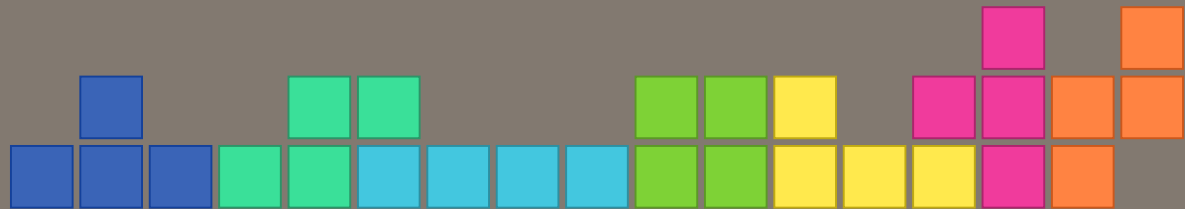


Why shouldn't you write your own crypto functions?

Implementing crypto algorithms is relatively easy

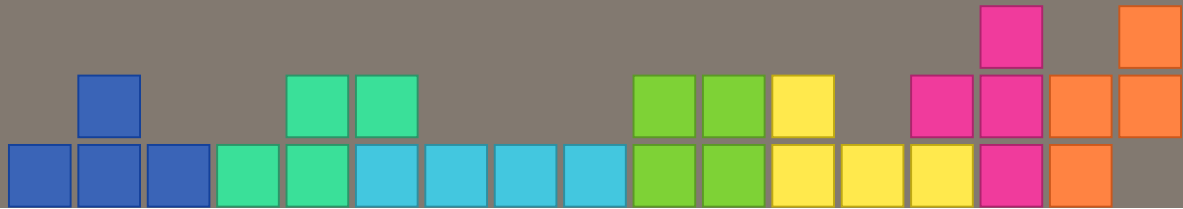
1. Preventing attacks on the implementation is hard
2. Writing secure and performant code is hard

Watch devconf.cz 2019 talk from Simo: Why you shouldn't write crypto functions yourself



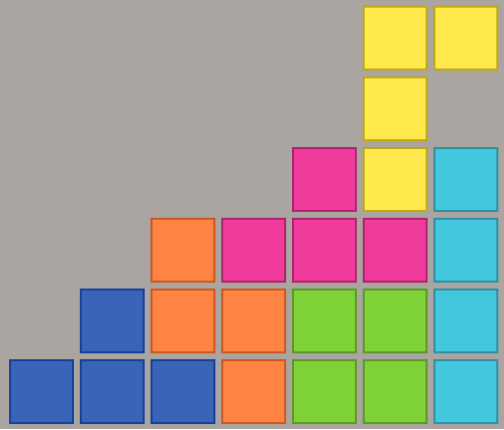
Why Samba shouldn't write its own crypto?

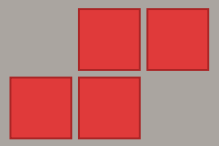
Samba developers aren't cryptographers



5

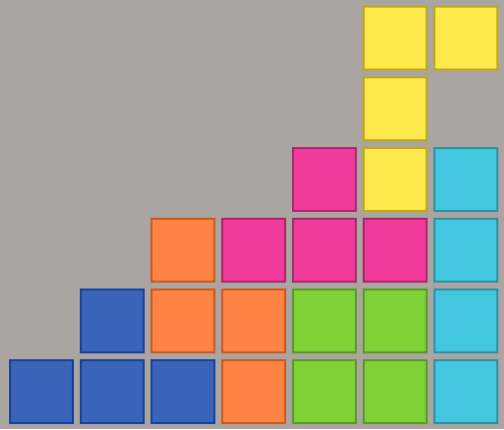
SMB3 and encryption





Samba and AES-NI support

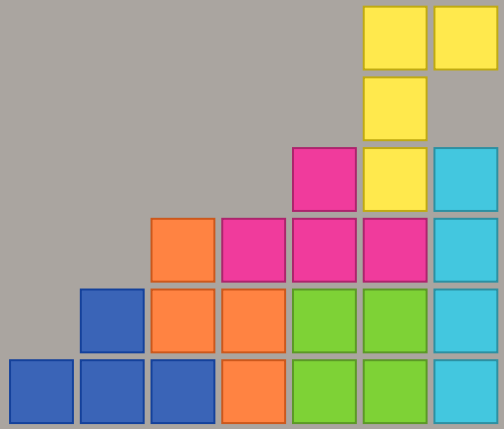
- AES-NI is hardware support for AES ciphers
- AES-NI is available on most hardware nowadays e.g. x86, ARM, SPARC T3
- Since Samba 4.8 we have support for Intel AES-NI on x86_64

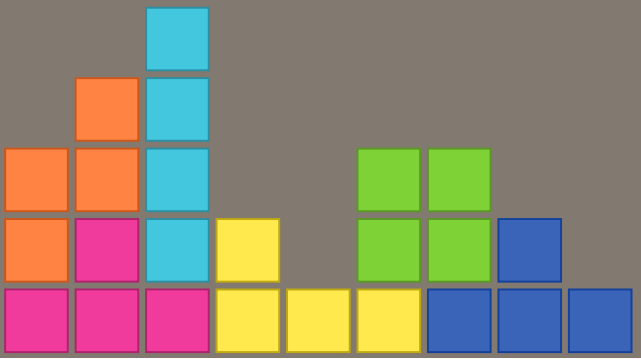


SMB3 encryption with AES-CCM/AES-GCM

For SMB3 encryption:

- Windows prefers AES-GCM over AES-CCM
- Samba perfers AES-CCM over AES-GCM

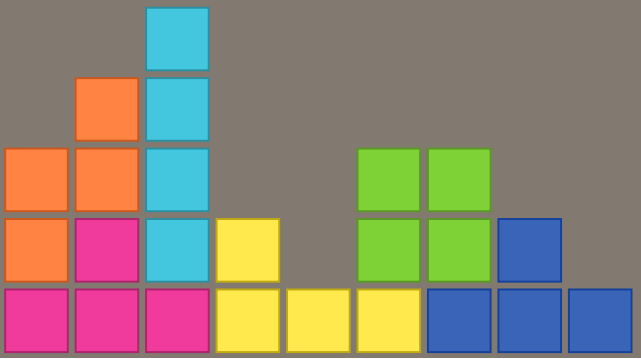




6

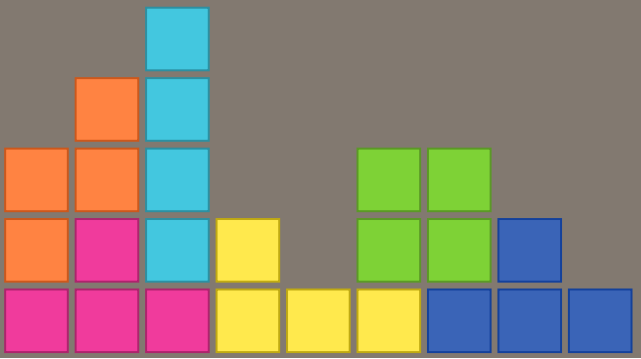
Numbers

Lets send and receive 1 GB of random data over SMB3 with encryption



Hardware

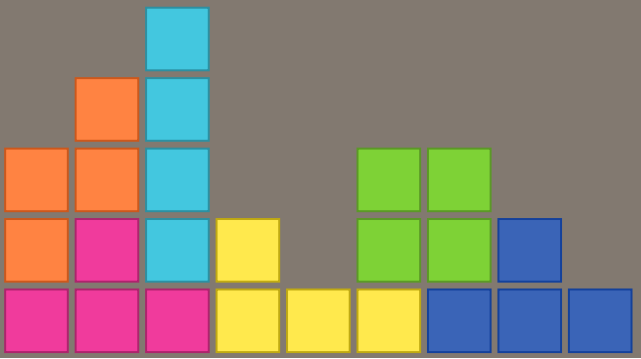
- CPU: i7-4960X CPU @ 3.60GHz (2013)
- RAM: 32GB
- Instruction Set: AES-NI support



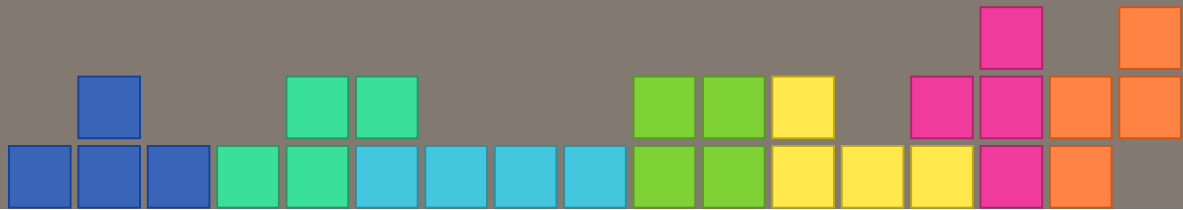
Send and receive 1 GB of random data over SMB3

```
time smbclient //LOCALSRV/tmp -mSMB3 -e \
  -c 'put 1GB.bin; get 1GB.bin /dev/null'
```

Client and server running at the same machine

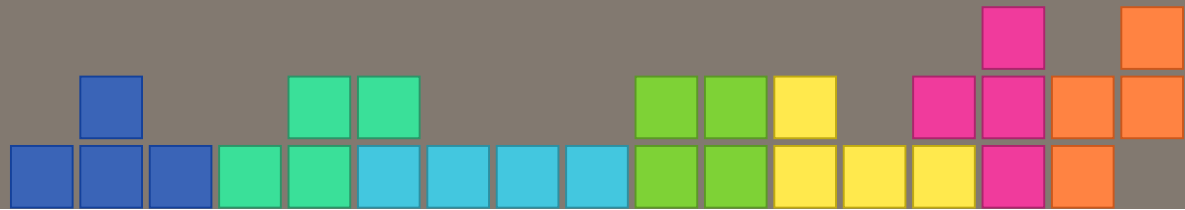


SMB3 Encryption with AES-CCM



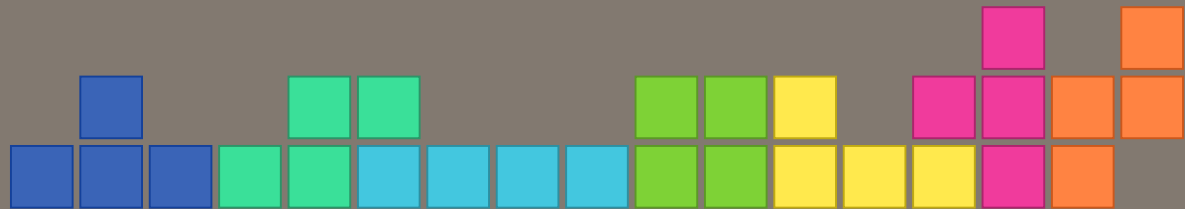
Samba 4.10 (AES-CCM)

```
putting file 1GB.bin (46458.8 kb/s) (average 46458.8 kb
getting file 1GB.bin (47832.1 kb/s) (average 47832.1 kb

real    0m44.613s
user    0m20.914s
sys     0m3.623s
```



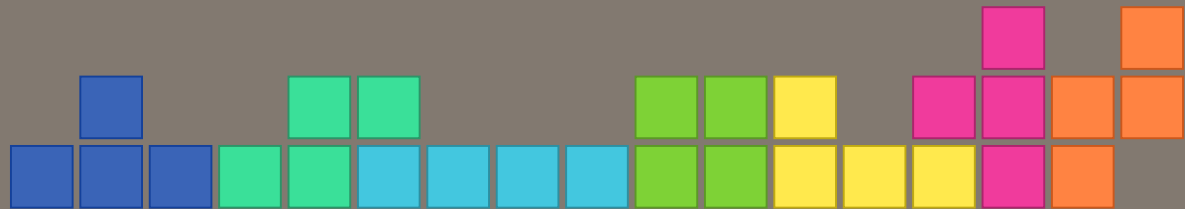
Samba 4.10, AES-NI (AES-CCM)

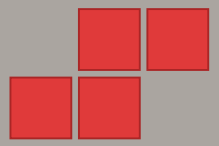
```
putting file 1GB.bin (88397.9 kb/s) (average 88397.9 kB
getting file 1GB.bin (90668.0 kb/s) (average 90668.1 kB

real    0m23.595s
user    0m10.427s
sys     0m3.694s
```



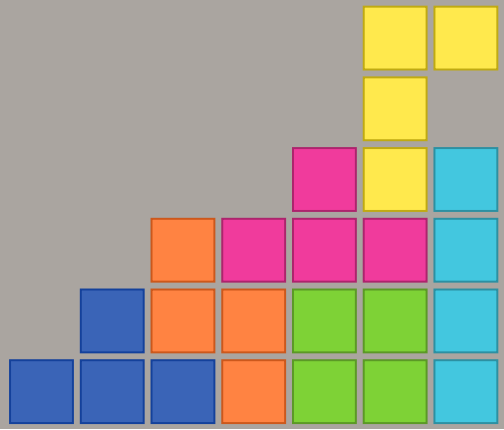
Samba with GnuTLS, AES-NI (AES-CCM)

```
putting file 1GB.bin (106747.0 kb/s) (average 106747.0
getting file 1GB.bin (110901.7 kb/s) (average 110901.7

real    0m19.454s
user    0m7.716s
sys     0m4.484s
```



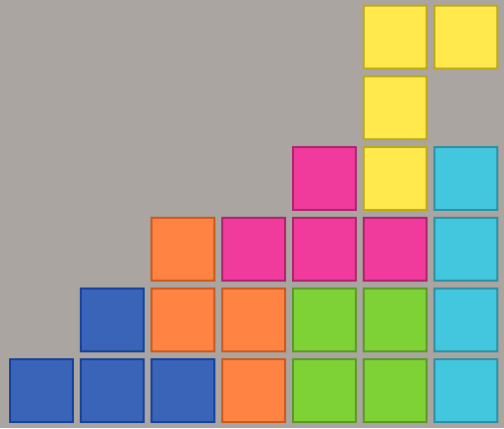


SMB3 Encryption with AES-GCM



Samba 4.10, AES-NI (AES-GCM)

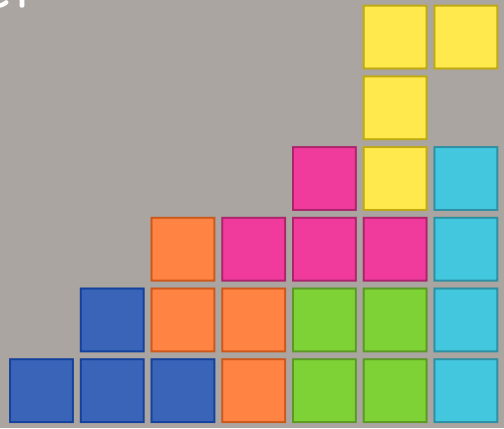
```
putting file 1GB.bin (3268.4 kb/s) (average 3268.4 kb/s
getting file 1GB.bin (3240.0 kb/s) (average 3240.0 kb/s

real    10m44.602s
user    5m21.525s
sys     0m3.820s
```



Samba with GnuTLS, AES-NI (AES-GCM)

```
putting file 1GB.bin (172010.5 kb/s) (average 172010.5
getting file 1GB.bin (183445.8 kb/s) (average 183445.8

real    0m12.299s
user    0m3.883s
sys     0m4.610s
```

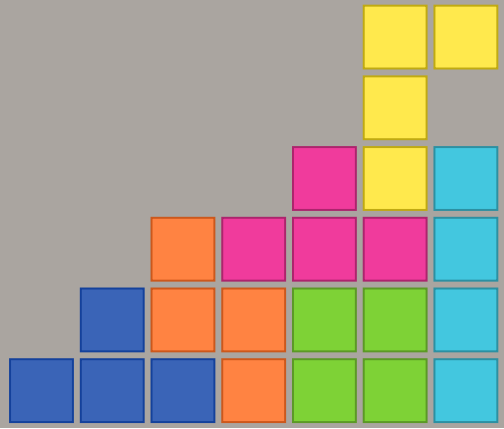
Speedup GCM: 50 times faster

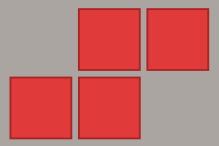


AES-CCM (Samba, AES-NI) vs AES-GCM (GnuTLS)

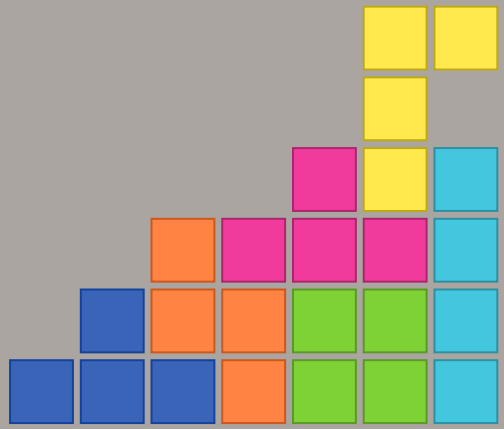
- AES-CCM (Samba 4.10): **23.454s (~90 MB/s)**
- AES-GCM (GnuTLS): **12.299s (~180 MB/s)**

Speedup: **Twice as fast**





Do you already start to love GnuTLS?

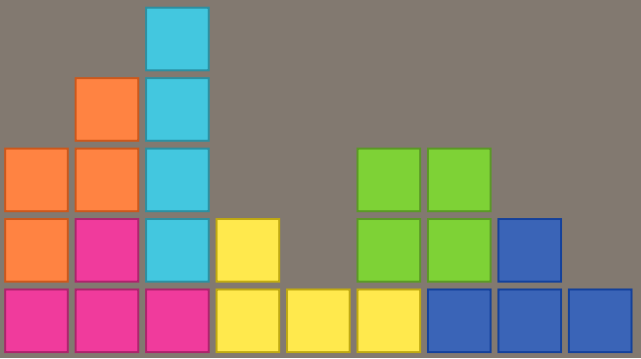


Signing with AES-CMAC

smbclient -mSMB3 --signing=required

- Samba crypto AES-NI: 0m15.239s
- Samba with GnuTLS: 0m14.833s

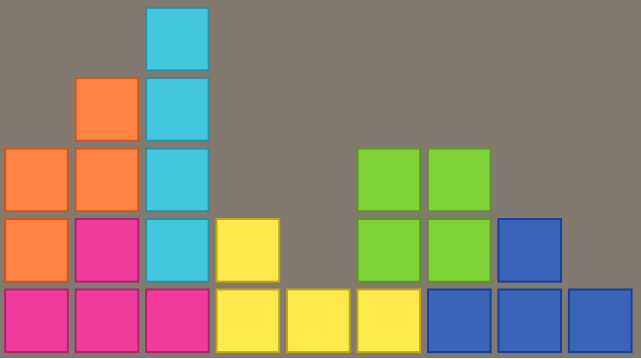
nettle implemented AES-CMAC based on Samba's implementation.



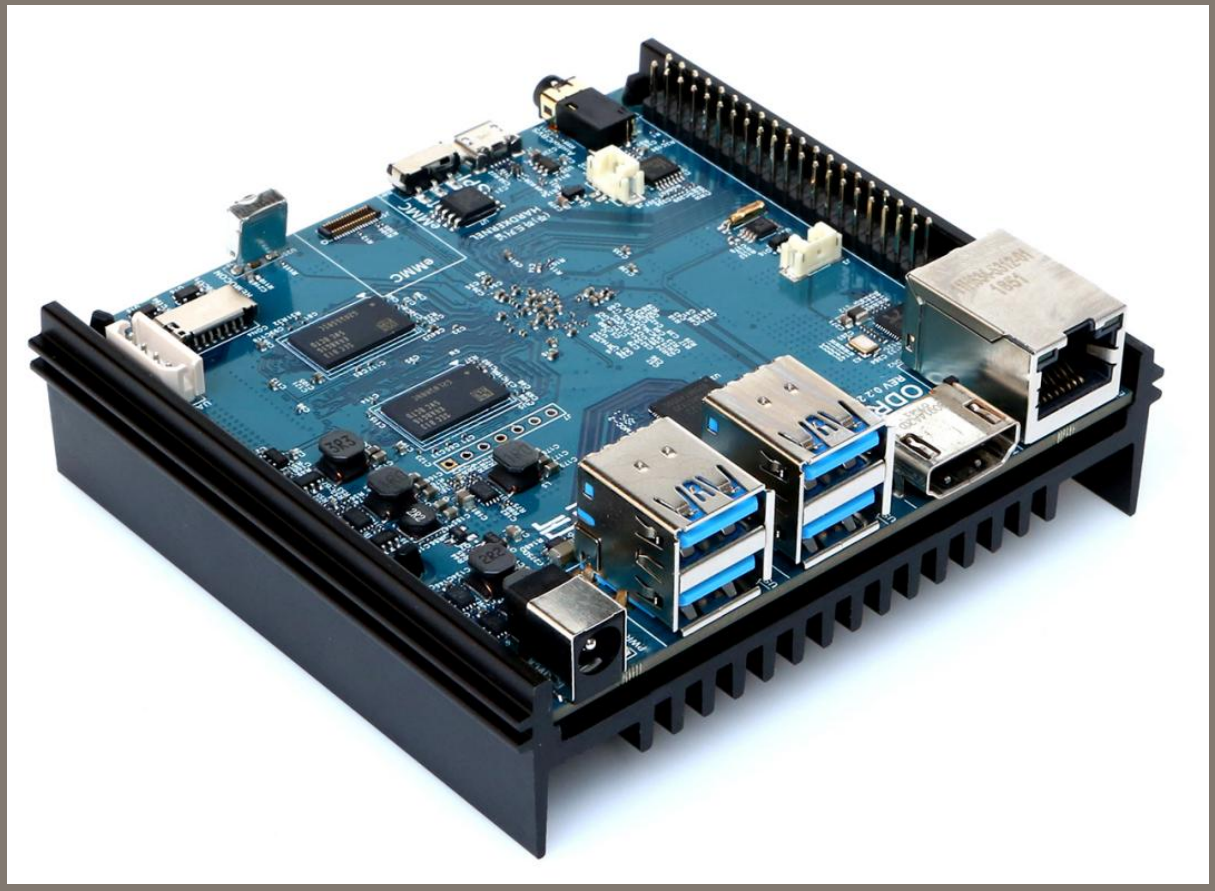
Signing with AES-GMAC (coming soon)

Will be introduced by Microsoft to SMB3 soon.

https://gitlab.com/gnutls/gnutls/issues/781

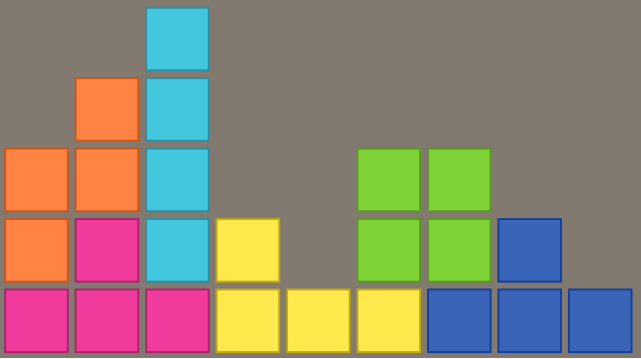


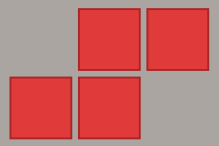
Next Hardware



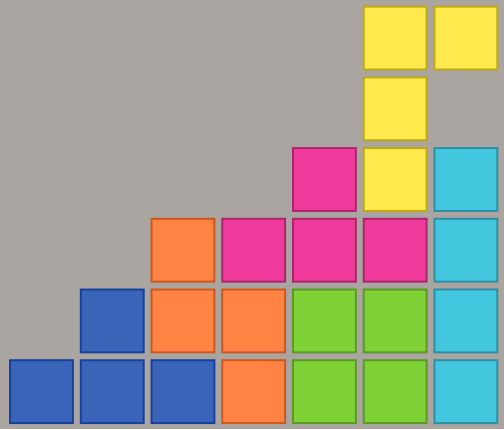
Hardkernel ODROID-N2

- ARM Cortex-A73 CPU (4 + 2 cores Cortex-A53)
- ARM64 with AES-NI support
- 4GByte DDR4 RAM
- Bad IO (~ 17MB/s) => tmpfs (ramdisk) for Samba share



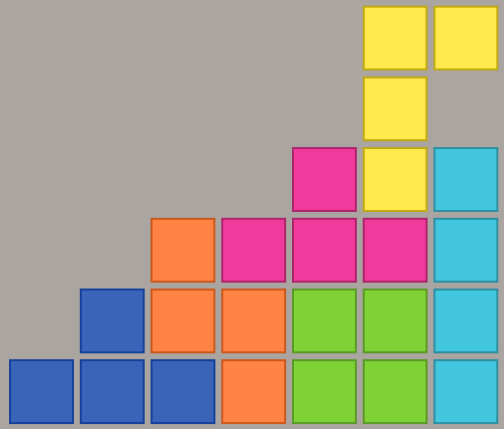


SMB3 Encryption with AES-CCM



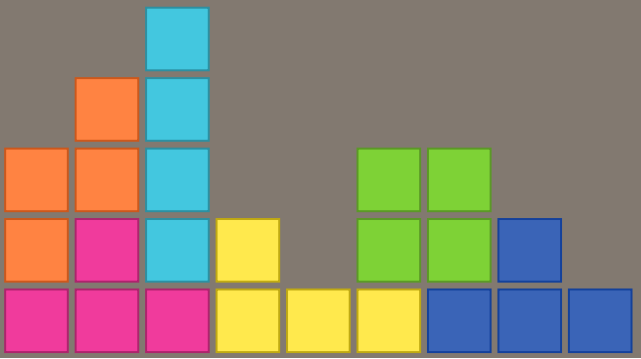
Samba 4.10 (AES-CCM)

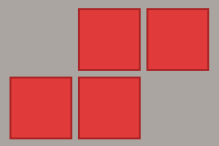
```
putting file 1GB.bin (13290.4 kb/s) (average 13290.4 kb
getting file 1GB.bin (14952.5 kb/s) (average 14952.5 kb

real    2m29.630s
user    1m2.436s
sys     0m20.992s
```



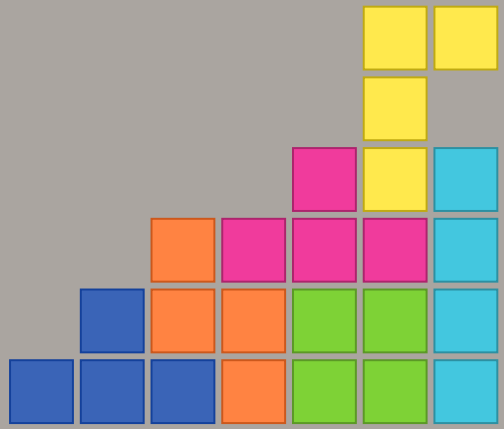
Samba with GnuTLS (AES-CCM)

```
putting file 1GB.bin (12714.6 kb/s) (average 12714.6 kB
getting file 1GB.bin (29526.5 kb/s) (average 29526.5 kB

real    1m58.512s
user    0m24.252s
sys     0m25.140s
```



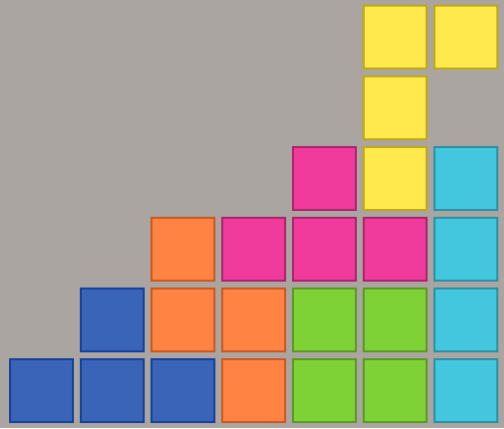


SMB3 Encryption with AES-GCM



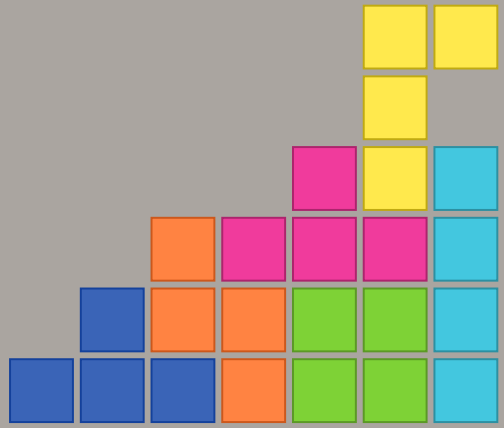
Samba 4.10 (AES-GCM)

```
putting file 1GB.bin (1372.8 kb/s) (average 1372.8 kb/s
getting file 1GB.bin (1370.0 kb/s) (average 1370.0 kb/s

real    25m29.725s
user    12m36.344s
sys     0m13.868s
```



Samba with GnuTLS (AES-GCM)

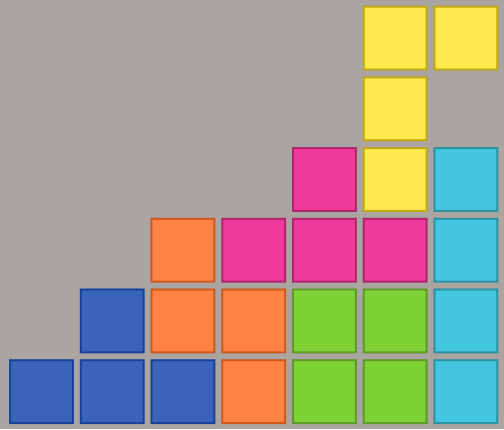
```
putting file 1GB.bin (23982.8 kb/s) (average 23982.8 kb
getting file 1GB.bin (37530.9 kb/s) (average 37530.9 kb

real    1m11.970s
user    0m18.504s
sys     0m23.932s
```



AES-CCM (Samba, AES-NI) vs AES-GCM (GnuTLS)

- AES-CCM (Samba 4.10): **149s (~14 MB/s**
- AES-GCM (GnuTLS): **71s (~37 MB/s)**

Speedup: **Twice as fast**

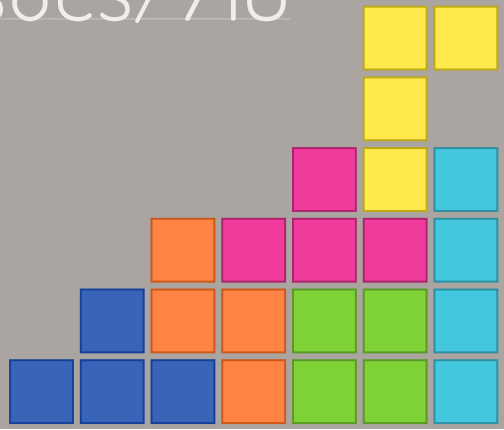


Performance will be even better when we get

```
gnutls_aead_cipher_(en|de)crypt_vec()
```

which uses io vectors.

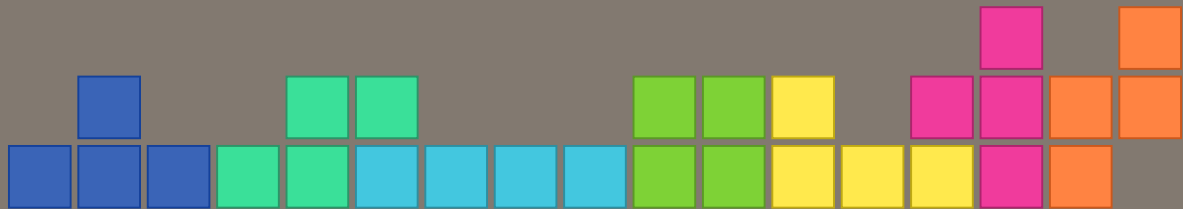
https://gitlab.com/gnutls/gnutls/issues/718



7

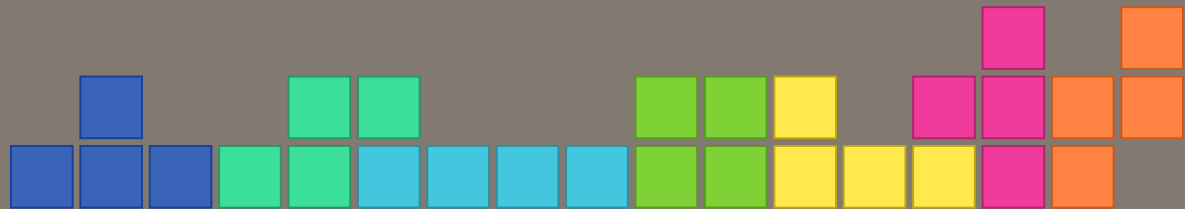
Lets talk about FIPS

Heinz Erhardt: Ritter FIPS



What is FIPS?

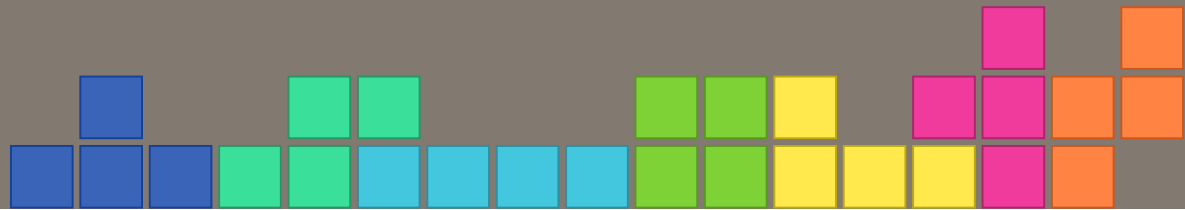
- Standard for Security Requirements for Cryptographic Modules by the US government
- Issued by the National Institute of Standards and Technology (NIST)



What is FIPS 140-2?

Set of requirements how to implement cryptography:

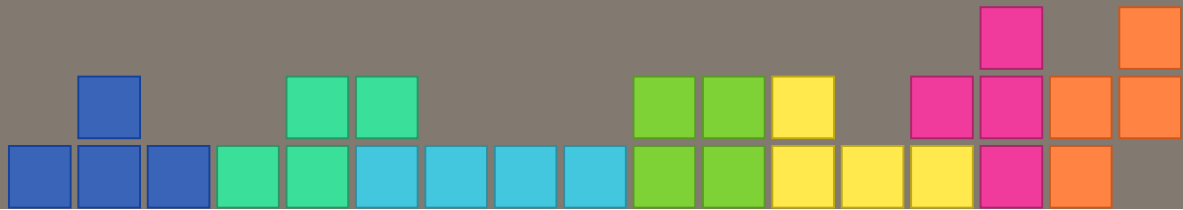
- Only use crypto algorithms and protocols only from a validated FIPS crypto library
- Ensure radom numbers are only coming from a validated FIPS crypto library



What is FIPS 140-2?

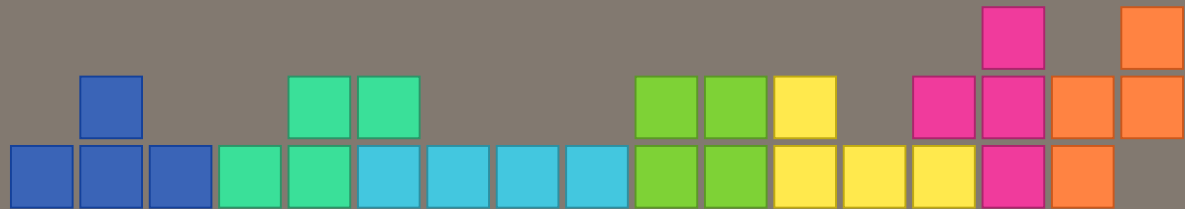
Set of requirements how to implement cryptography:

- Check whether only approved or allowed crypto algorithms are used for security relevant functionality
- Secret keys and other secret material must be zeroized once it is no longer used



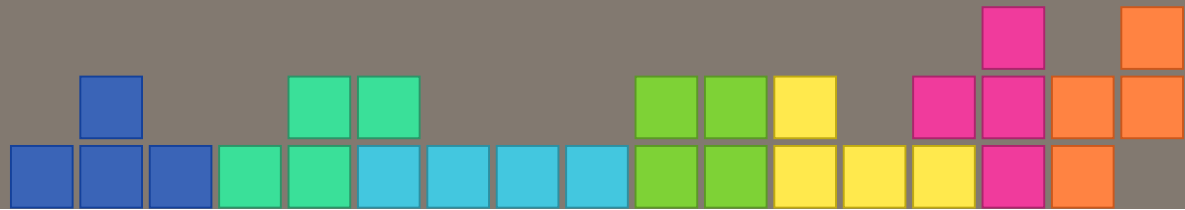
For FIPS mode:

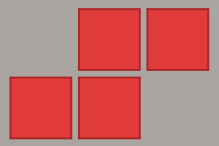
- Kernel boots with a special command line option (fips=1)
- Or you set: `echo 1 > /etc/system-fips`
- Based on those option crytpo implementations only allow to use a certain set of ciphers and hashes



What does FIPS 140-2 mean for Samba?

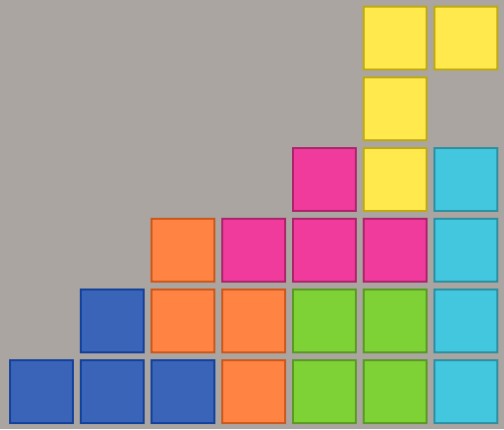
- RC4 and MD5 is not available
  1. NTLM doesn't work, only KRB5
  2. SMB1 doesn't work (only guest connections)





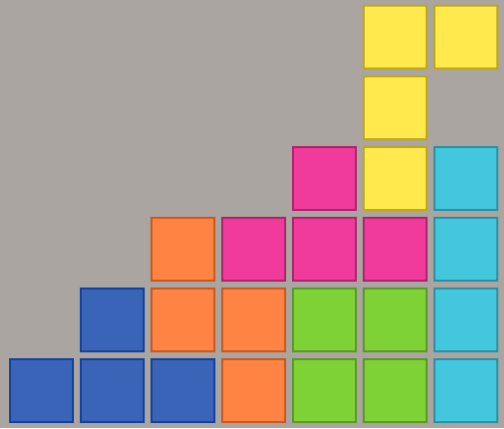
8

Requriements



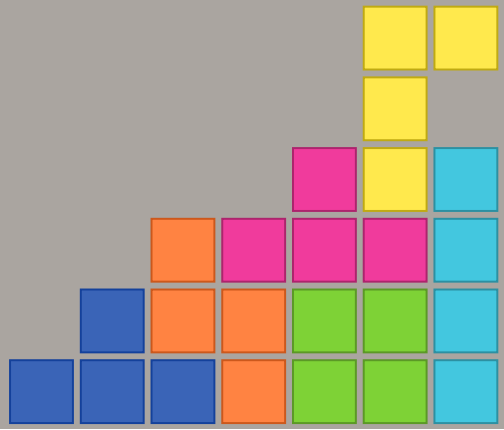
Requirements for GnuTLS

- Minimum requirement: **GnuTLS 3.2**
- For AES-GCM and AES-CCM: **>= 3.4.7**
- For AES-CMAC and AES-CFB8: **>= 3.6.5**
- For FIPS mode: **>= 3.6.6**



Release?

October 2019 - Samba 4.11



GAME OVER