

Electronic **C**oloring **B**ook **L**et's break some crypto with...



Your mission

Break an image encrypted with “**AES-128 ECB**”

Your mission

Break an image encrypted with “**AES-128 ECB**”

AES = *Advanced Encryption Standard*

Your mission

Break an image encrypted with “**AES-128 ECB**”

AES = *Advanced Encryption Standard*

128 = There are $2 \times 2 \times 2 \times 2 \times \dots$ (count 128) $\dots \times 2$

Your mission

Break an image encrypted with “**AES-128 ECB**”

AES = *Advanced Encryption Standard*

- 128** = There are $2 \times 2 \times 2 \times 2 \times \dots$ (count 128) $\dots \times 2$
- = 340282366920938463463374607431768211456 possible keys
- = 340 Millions of Millions of Millions of Millions of Millions

Your mission

Break an image encrypted with “**AES-128 ECB**”

AES = *Advanced Encryption Standard*

128 = There are $2 \times 2 \times 2 \times 2 \times \dots$ (count 128) $\dots \times 2$
= 340282366920938463463374607431768211456 possible keys

ECB = *Electronic Code Book*

or maybe *Electronic Coloring Book?*

No crypto toy, kids, it's real!

Addonics Product: Di

www.addonics.com/products/dchd256e.php

Storage Systems ▶ Storage Products ▶ Sales ▶ Support ▶ About ▶

Home > Drive Cartridge System > Combo Hard Drive > Diamond Cipher Combo HDD for SATA hard drive with eSATA or USB 3.0/2.0 External Connection

Diamond Cipher Combo HDD for SATA hard drive with eSATA or USB 3.0/2.0 External Connection



Overview Features Specifications Model and Price Support

DIAMOND CIPHER COMBO HARD DRIVE

Diamond drive enclosure
eSATA connector
On/Off switch
Connect to 12V power adapter

Rear View of Diamond Cradle
click for detailed view

SATA connection to motherboard
Diamond Drive Cradle
Power LED
Drive Activity LED
Cipher key
Removable front bezel and optional cooling fan
Cradle lock and power switch

The Diamond Cipher Combo Hard Drive Kit features the new generation of eSATA hard drive enclosures with the 256-bit AES hard encryption and choice of [ECB or CBC](#) mode. The encryption is FIPS certified to ensure absolute data security should the drive get stolen or lost. The crypto engine inside the Diamond Cipher enclosure handles all the encryption and decryption on the fly with no detectable performance degradation on data transfer. Using native eSATA interface, the Diamond Cipher Combo Hard Drive supports the highest performance possible today through an externally connected hard drive enclosure.

The Diamond Combo Hard Drive kit is probably the most versatile storage solution in the market. This kit comes with all the necessary component to allow any 3.5" SATA hard drive to be used as a drive cartridge and as an external high performance eSATA hard drive. Constructed in heavy gauge aluminum with precision finish for smooth operation, the Diamond Cipher drive kit is built to last while at the same time providing excellent heat dissipation for the hard drive. Comes built in with the Addonics SATA direct bridge interface, the Diamond Cipher drive enclosure allows the SATA hard drive to appear as a direct connection to the host both in eSATA mode or SATA mode while at the same time isolates the SATA hard drive power and data connectors from the wears and tears incurred in some of the removable SATA hard drive system. 2.5" SATA hard drive can also be installed into the Diamond Cipher drive enclosure using the optional [2.5" hard drive mounting bracket](#).

Model:
DCHD256EU3 - \$145.00

Shop Online

No crypto toy, kids, it's real!

The screenshot shows a web browser displaying the Addonics website at www.addonics.com/products/dchd256e.php. The page features the Addonics Technologies logo and navigation links for Storage Systems, Storage Products, Sales, Support, and About. A search bar and an 'Online Store' button are also present. The main content area displays the 'Diamond Cipher Combo HDD' product, highlighting its FIPS certification and AES encryption capabilities. Two images of the drive are shown: one in its enclosure and another showing the internal components. A large blue callout box contains several red annotations from the user.

Diamond Cipher Combo HDD

SATA
USB

[...] **AES hard encryption and choice of ECB or CBC mode.**
The encryption is FIPS certified to ensure **absolute data security**
should the drive get stolen or lost [...]

[...] **To hack into ECB encryption [...] the computational power**
requires to derive this actual key is simply phenomenal.

The Diamond Cipher Combo Hard Drive Kit features the new generation of...
encryption and choice of [ECB or CBC mode](#). The encryption is FIPS certified to ensure absolute data security...
or lost. The crypto engine inside the Diamond Cipher enclosure handles all the encryption and decryption on the fly with no detectable...
performance degradation on data transfer. Using native eSATA interface, the Diamond Cipher Combo Hard Drive supports the highest...
performance possible today through an externally connected hard drive enclosure.

The Diamond Combo Hard Drive kit is probably the most versatile storage solution in the market. This kit comes with all the necessary...
component to allow any 3.5" SATA hard drive to be used as a drive cartridge and as an external high performance eSATA hard drive.
Constructed in heavy gauge aluminum with precision finish for smooth operation, the Diamond Cipher drive kit is built to last while at the...
same time providing excellent heat dissipation for the hard drive. Comes built in with the Addonics SATA direct bridge interface, the...
Diamond Cipher drive enclosure allows the SATA hard drive to appear as a direct connection to the host both in eSATA mode or SATA...
mode while at the same time isolates the SATA hard drive power and data connectors from the wears and tears incurred in some of the...
removable SATA hard drive system. 2.5" SATA hard drive can also be installed into the Diamond Cipher drive enclosure using the...
optional [2.5" hard drive mounting bracket](#).

Model:
DCHD256EU3 - \$145.00

Shop Online



Absolute data security?

We have a secret weapon!



AES is a block cipher:



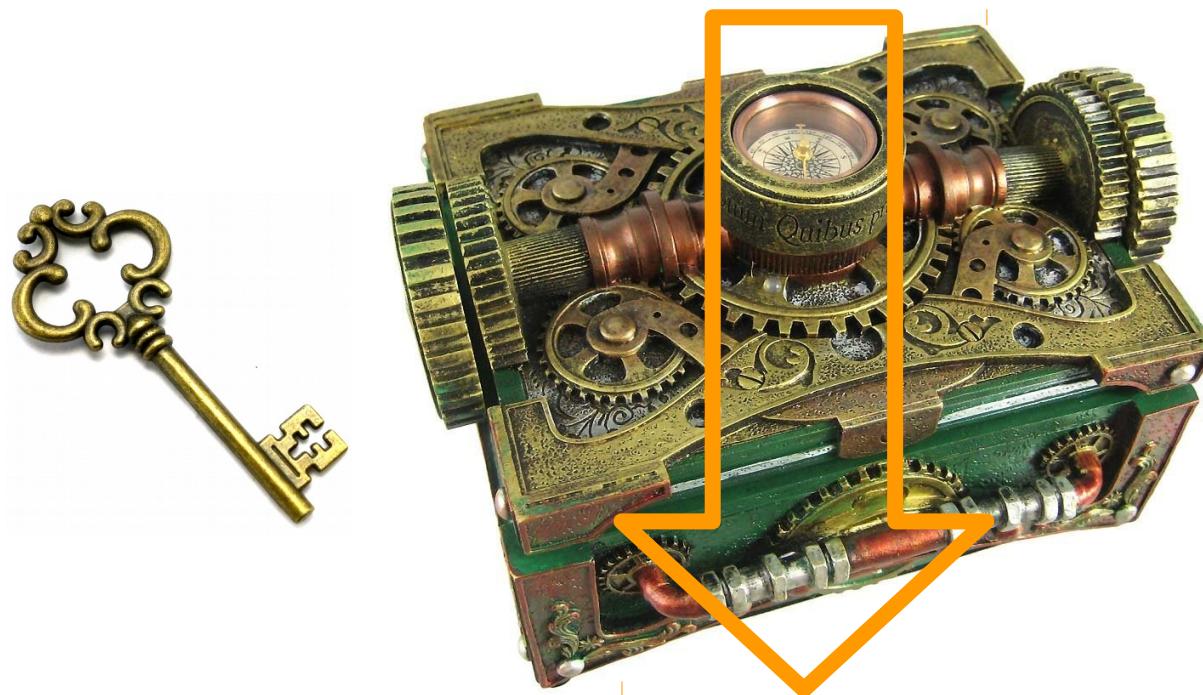
M₃ I₁ S₁ S₁ Y₄ O₁ U₁



M₃ I₁ S₁ S₁ Y₄ O₁ U₁



M₃ I₁ S₁ S₁ Y₄ O₁ U₁

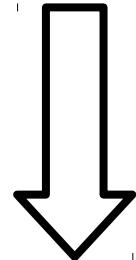


J₈ G₂ R₁ F₄ K₅ L₁ L₁

a block of text.

+

MySecretKey12345



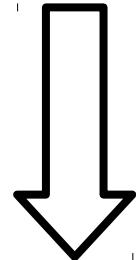
7 ←n≡i | *←∞ L F • i û→

(bf 11 6e ca 69 de 0f 1b ec c0 c6 f9 69 96 d0 10)

a block of text.

+

MySecretKey12346



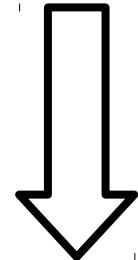
7 ←n||i | ☀←∞ L ↳• i û||→

(bf 11 6e ca 69 de 0f 1b ec c0 c6 f9 69 96 d0 10)

a block of text.

+

MySecretKey12346



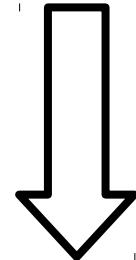
g0+7 ÑëØcë VLÇk||î

(67 4f c5 bb a5 89 ea 63 89 20 1f 4c 80 6b d0 8c)

a block of text?

+

MySecretKey12346



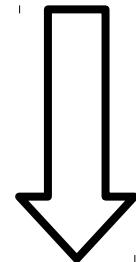
g0+¶ ÑëØcë VLÇk¶î

(67 4f c5 bb a5 89 ea 63 89 20 1f 4c 80 6b d0 8c)

a block of text?

+

MySecretKey12346



♣m♦O¬¬jF∫æ∫■²±♪ç

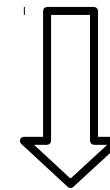
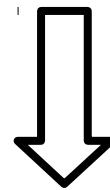
(05 6d 04 4f bf a9 6a 46 f4 91 f4 dc fd cf 0d 87)

Yeah, but my message is larger!
How to encrypt more than one block?

My secret message won't fit here

How to encrypt more than one block?

My secret message won't fit here



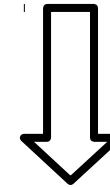
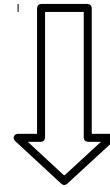
How to encrypt more than one block?

My secret message won't fit here

+

+

MySecretKey12345MySecretKey12345



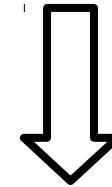
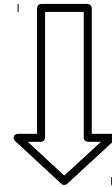
How to encrypt more than one block?

My secret message won't fit here

+

+

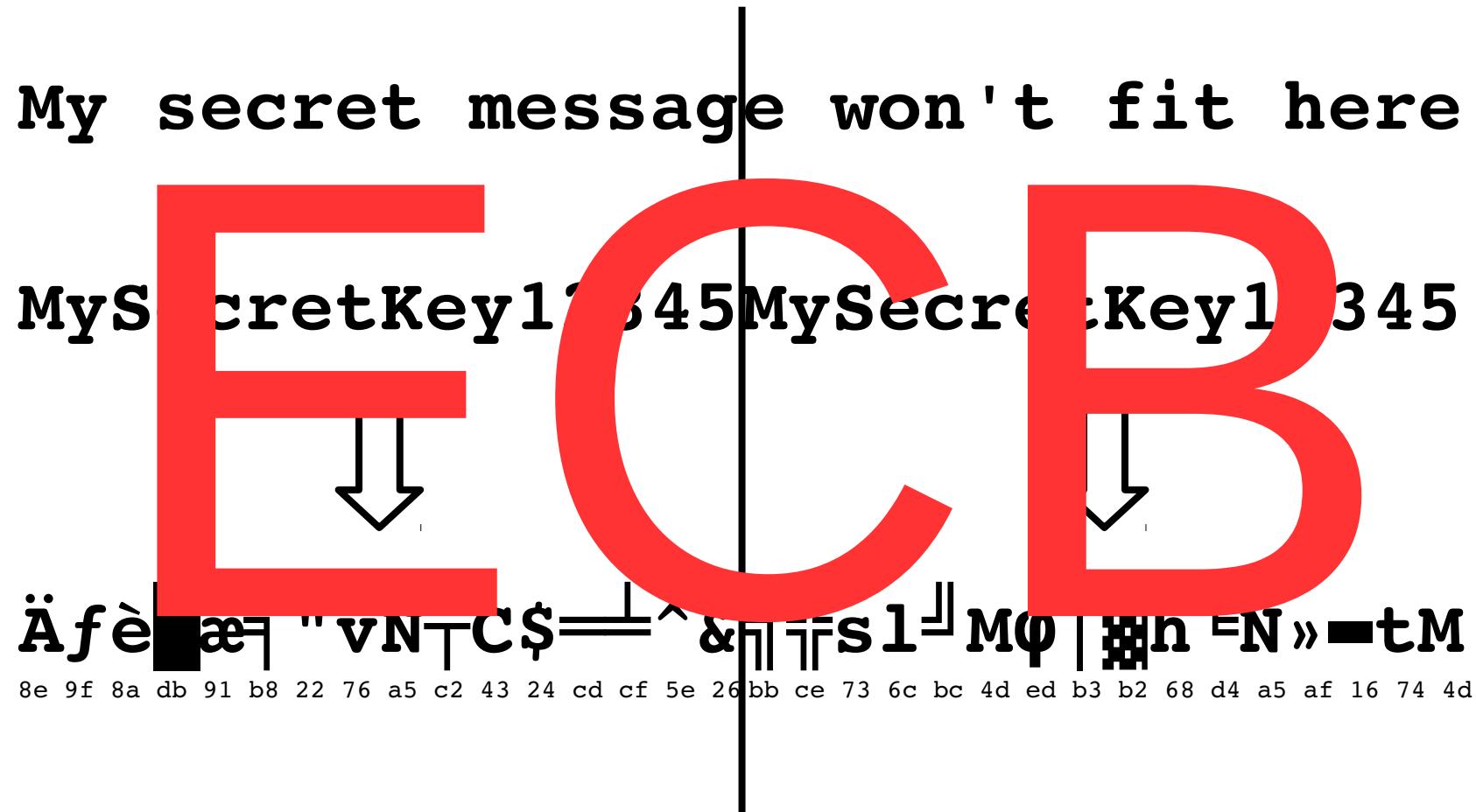
MySecretKey12345MySecretKey12345

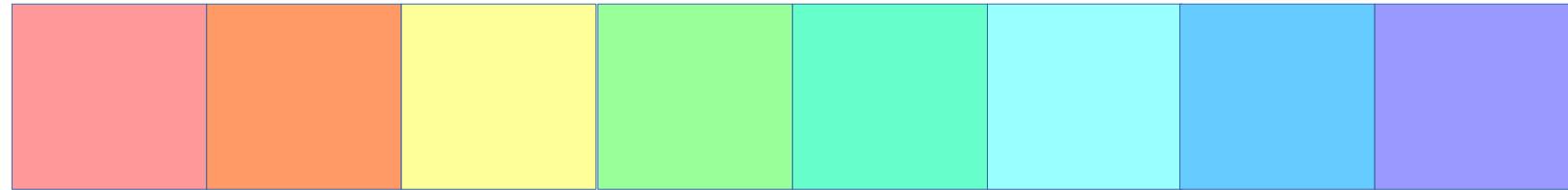


Äfè█æ█ "vÑTc\$=└^&███s1└Mφ | ███h LÑ»—tM

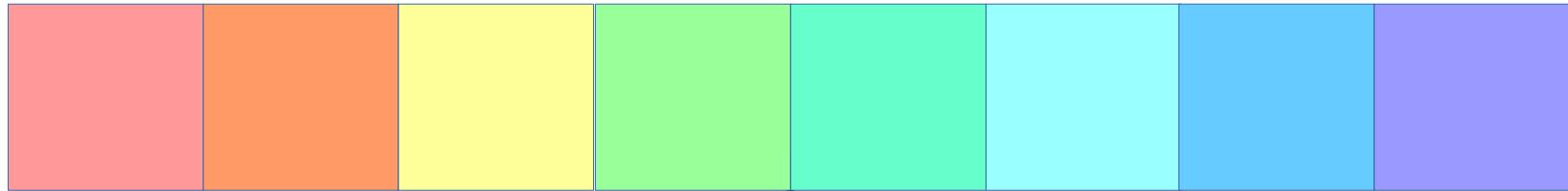
8e 9f 8a db 91 b8 22 76 a5 c2 43 24 cd cf 5e 26 bb ce 73 6c bc 4d ed b3 b2 68 d4 a5 af 16 74 4d

How to encrypt more than one block?





FF9999FF FF9966FF FFFF99FF 99FF99FF 66FFCCFF 99FFFFFF 66CCFFFF 9999FFFF

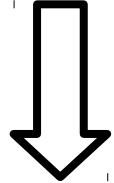


FF9999FF FF9966FF FFFF99FF 99FF99FF

66FFCCFF 99FFFFFF 66CCFFFF 9999FFFF

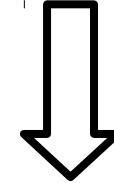
+

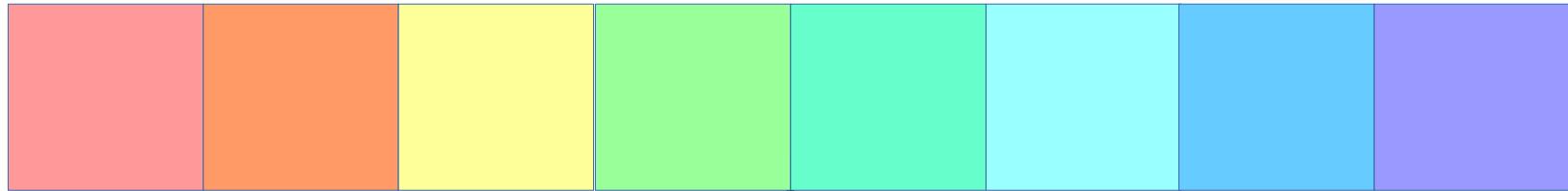
MySecretKey12345



+

MySecretKey12345

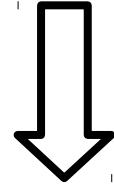




FF9999FF FF9966FF FFFF99FF 99FF99FF

+

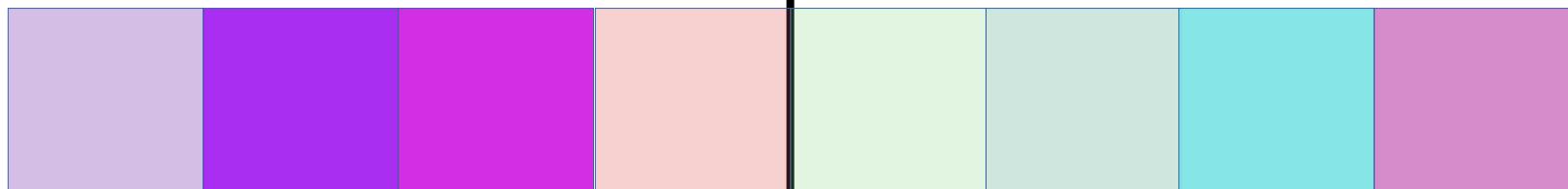
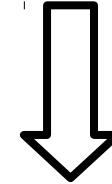
MySecretKey12345



66FFCCFF 99FFFFFF 66CCFFFF 9999FFFF

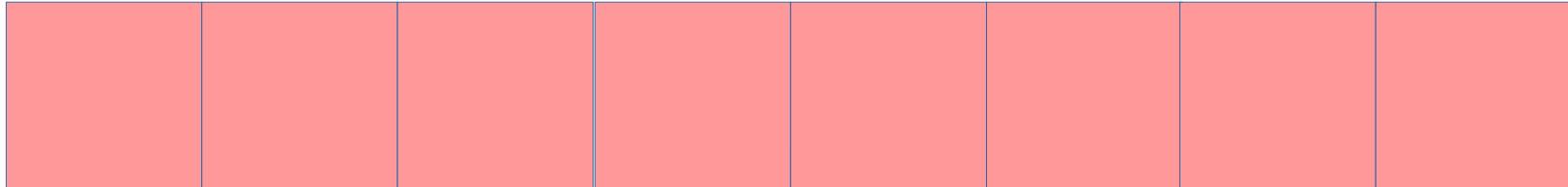
+

MySecretKey12345



af87d189 a51ff2f1 d025ecf5 dd42383e

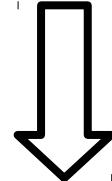
7cd47a39 54a78947 7de4e5ed c251b1aa



FF9999FF FF9999FF FF9999FF FF9999FF | FF9999FF FF9999FF FF9999FF FF9999FF

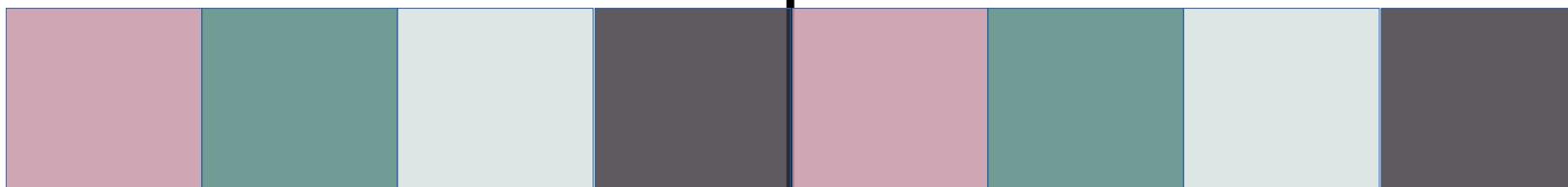
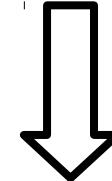
+

MySecretKey12345

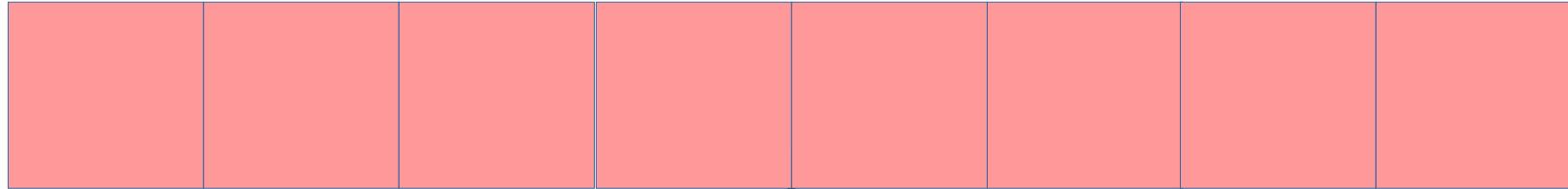


+

MySecretKey12345



c798a7da 05514593 b7cdcc81 393339cf | c798a7da 05514593 b7cdcc81 393339cf



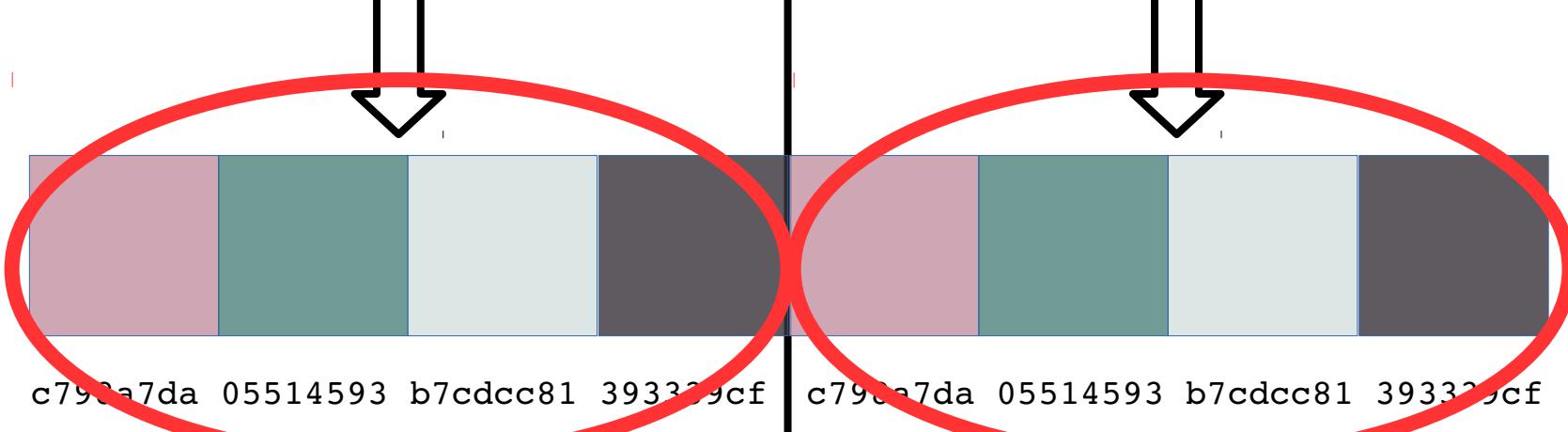
FF9999FF FF9999FF FF9999FF FF9999FF | FF9999FF FF9999FF FF9999FF FF9999FF

+

MySecretKey12345

+

MySecretKey12345





Can we do better?

Repeating blocks

= very probably uniform color

→ Paint them!





Your turn!

You got an encrypted file.

ary-grade AES-128 crypto!



61df505ad423f5b5 a8b9f9263d42bea9	7d3b369024952975 596bb4a98d422b6a	37db73ca34e392c2 9f81179565ac49a2	f37c4cd2af2fa267 09c55383a2f1eab1	021bc43df0dd5 32cf6fd900e8a
7d3b369024952975 596bb4a98d422b6a	7d3b369024952975 596bb4a98d422b6a	7d3b369024952975 596bb4a98d422b6a	51f4b0a0e32b5c54 bc2e92a0115297ec	22cc270be24e9 7591dc6cf31aa

Your turn!

You got an encrypted file.

- 1) Find a set of repeating blocks.

ary-grade AES-128 crypto!



61df505ad423f5b5 a8b9f9263d42bea9	7d3b369024952975 596bb4a98d422b6a	37db73ca34e392c2 9f81179565ac49a2	f37c4cd2af2fa267 09c55383a2f1eab1	021bc43df0dd5 32cf6fd900e8a
7d3b369024952975 596bb4a98d422b6a	7d3b369024952975 596bb4a98d422b6a	7d3b369024952975 596bb4a98d422b6a	51f4b0a0e32b5c54 bc2e92a0115297ec	22cc270be24e9 7591dc6cf31aa

Your turn!

You got an encrypted file.

- 1) Find a set of repeating blocks.

ary-grade AES-128 crypto!



61df505ad423f5b5 a8b9f9263d42bea9	7d 59	37db73ca34e392c2 9f81179565ac49a2	f37c4cd2af2fa267 09c55383a2f1eab1	021bc43df0dd5 32cf6fd900e8a
7d 59	7d 59	7d 59	51f4b0a0e32b5c54 bc2e92a0115297ec	22cc270be24e9 7591dc6cf31aa

Your turn!

You got an encrypted file.

- 1) Find a set of repeating blocks.
- 2) Paint them with the color of your choice!

ary-grade AES-128 crypto!



61df505ad423f5b5 a8b9f9263d42bea9	7d3b369024952975 596bb4a98d422b6a	37db73ca34e392c2 9f81179565ac49a2	f37c4cd2af2fa267 09c55383a2f1eab1	021bc43df0dd5 32cf6fd900e8a
7d3b369024952975 596bb4a98d422b6a	7d3b369024952975 596bb4a98d422b6a	7d3b369024952975 596bb4a98d422b6a	51f4b0a0e32b5c54 bc2e92a0115297ec	22cc270be24e9 7591dc6cf31aa

Your turn!

You got an encrypted file.

- 1) Find a set of repeating blocks.
- 2) Paint them with the color of your choice!
- 3) Other set(s) of repeating blocks?
Paint them too with other color(s)!

So, what's the secret image?

Some slides were shamelessly inspired by



by Ange Albertini

<https://speakerdeck.com/ange/lets-play-with-crypto-v2>

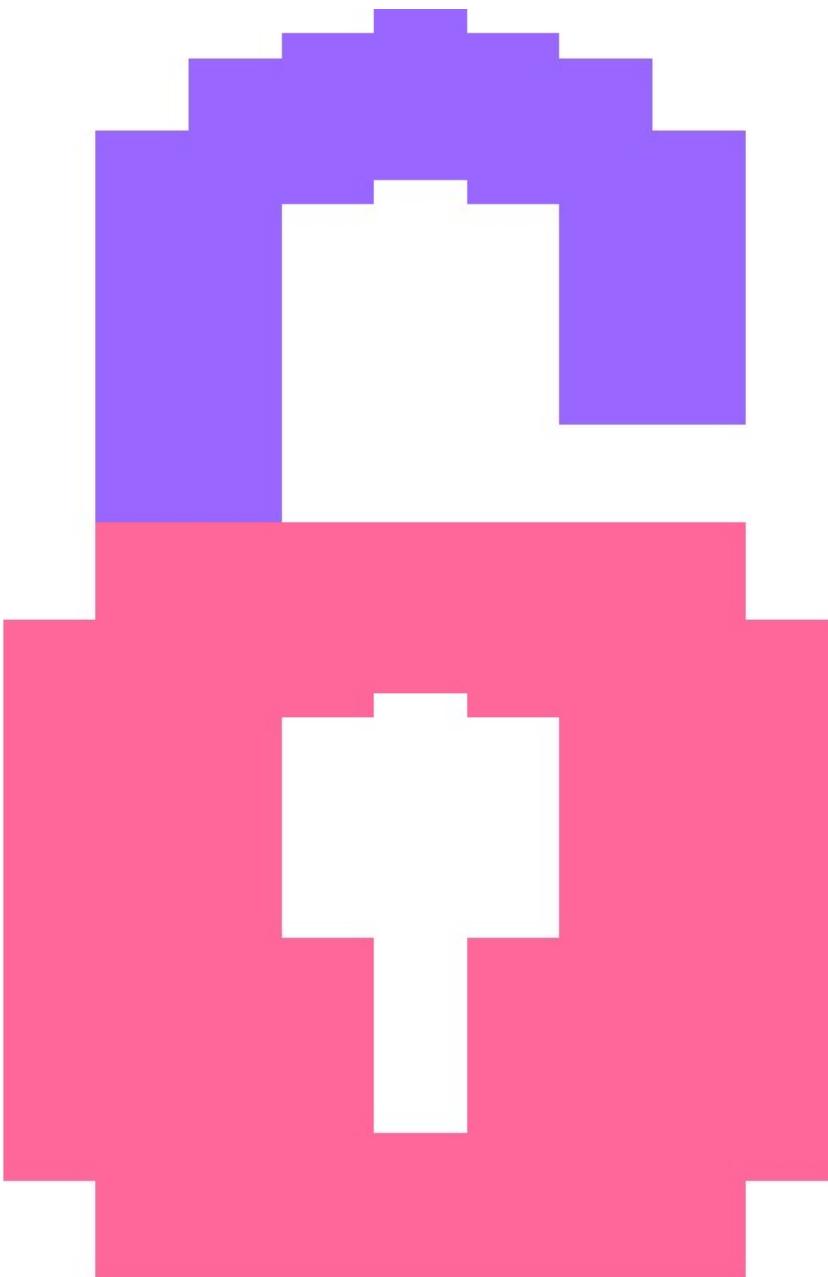
<https://www.youtube.com/watch?v=bcxF6IYTCg0>

Thank You

TapadhLeat Köszönöm Murakoze
Shukriya Buznyg WaadMahadsantahay FaafetaiLava Ngiyabonga
ThintKo TapadhLeibh AsanteSana Waila
Blagodaram Rahmat Welatin TangioTumas Dhanyarad
Matondo Matumun Tahan Sukiya
Merce Mercé Tanaan KeyLeboha
Taiku Dankon aNIKé Nizzik ajr Aguyjé
Dakujem Blagodaria Grandmercé Dhanyavadalu Sulpay
Gràcies Blagodari Faleminderit Merkzi Akun
Efharisto Mehbarani
Näjistuke Hvala Arigatō Obrigado
Grandmercé Dhanyavadalu Sulpay
Nandri Spas
Mehbarani ÇoxSagOlun Nirringrazzjak Bayarlalaa
Mahalo Gracinas DankJuWel
DankJuWel Marahaba Diky TakkFyri
Wado Salamat
Asante KamSahHamnida Saha Multumesc
Rahmet
Danke
Padies
ANIKé
Misaotra
MaloTeOfa
Akpé
Gracie
Cámon
Gracie
Tak
Sagolun
Ačiū
Dankie
TánanVäga
Khobchajdeu
Trugére
Chnorakaloutioum
Milesker
Yekeniele
Barkal KurreSumanga
Mauruuru KyayTzuTinPaTe
GoRaibhMaithAgat Mochchakkeram
GraciasAgimus Dhanyabaad
Akiiba
KopKhunKha
Motashakkeram

TIFF file encrypted with military-grade AES-128 crypto!

TOP SECRET



fdd65 8dc9c9cb99 6ba bc-8 ec2ad7d7-12ba8b 96fa5a1fe ac217ac65 2 8d715e5 4de7d5e59 5cad 96 8ec65117ec 8e3ca280 6-ae7-62e-6bc5a5af 77 ecbf efcfcfb5 15e9 d 8ee97bd2 5d6 9f77

TIFF file encrypted with military-grade AES-128 crypto!

TOP SECRET

