SUNDAY 26 MARCH 2017 (2017-03-26) | Unknown author

VolgaCTF 2017 Quals - VC - Crypto

Informations

Version

By	Version	Comment
noraj	1.0	Creation

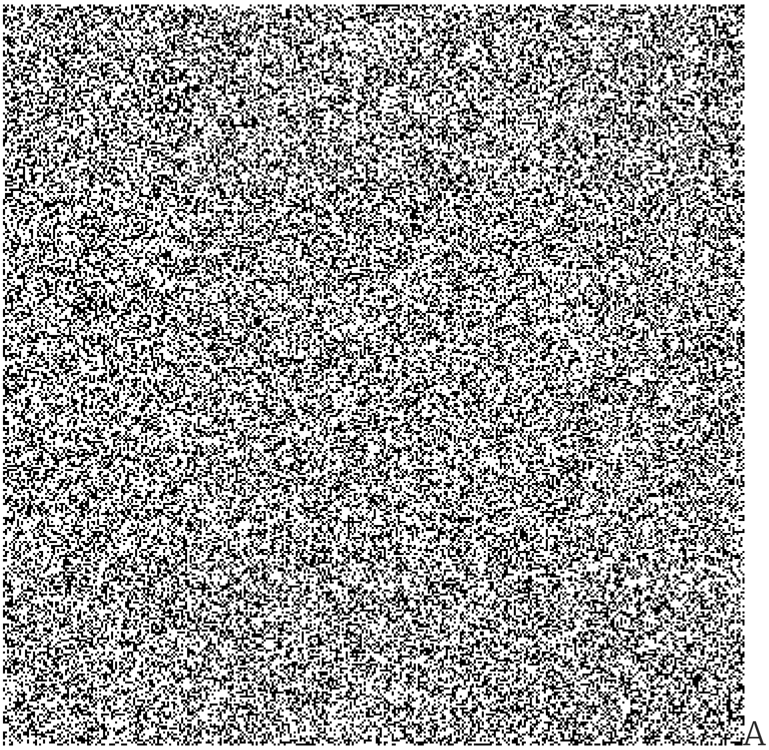
CTF

- **Name** : VolgaCTF 2017 Quals
- **Website** : quals.2017.volgactf.ru
- **Type** : Online
- **Format** : Jeopardy
- **CTF Time** : link

Description

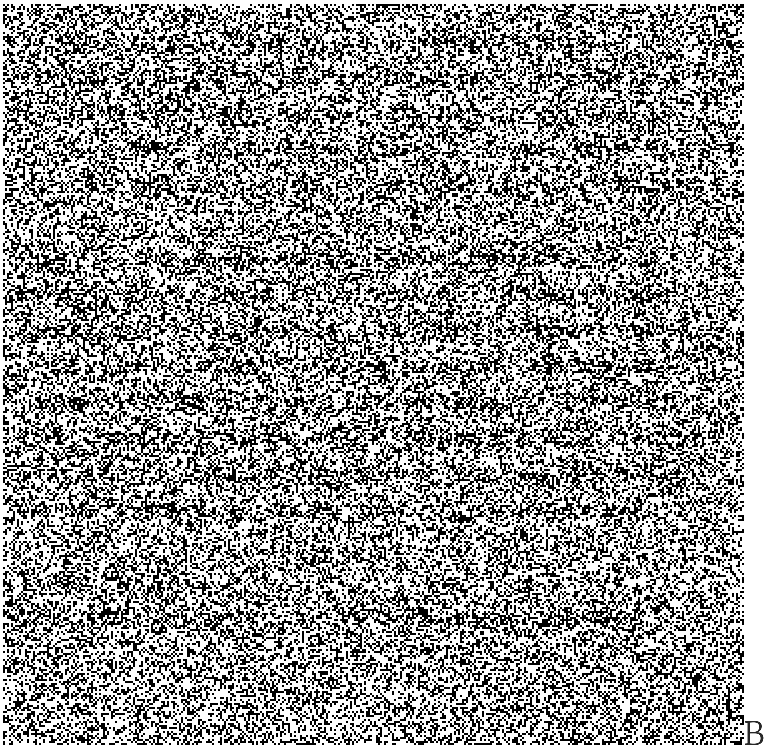
> There are files A.png and B.png. But where's the flag?
>
> A.png
>
> B.png

A.png:



A

B.png:



B

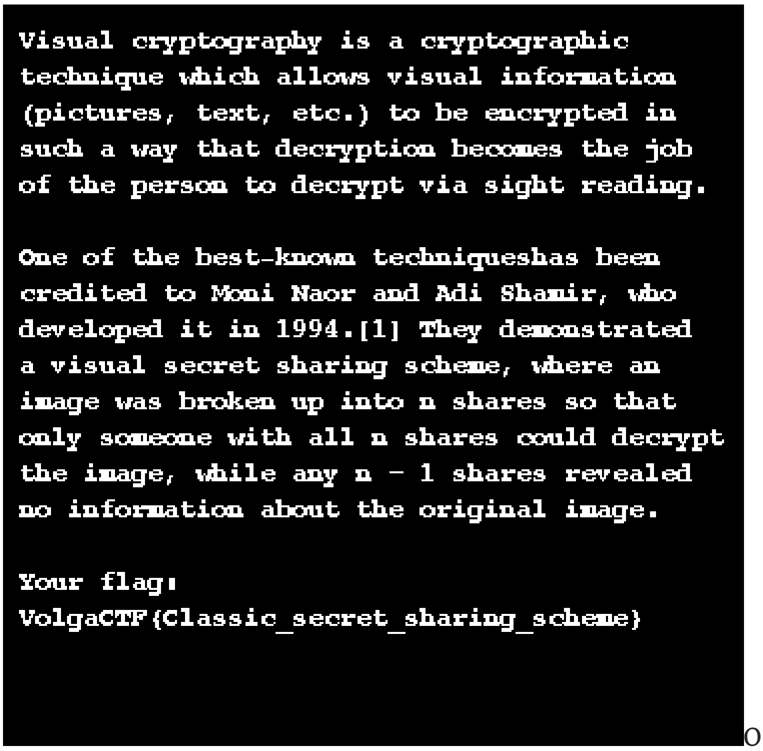
Solution

If you know OTP you must know this famous attack on pad reused.

You can also see some black lines on image B. Now let's XOR image A and B (with ImageMagick):

```
$ convert A.png B.png -fx "(((255*u)&(255*(1-v)))|((255*(1-u))&(255*v)))/255" out.png
```

And now we get the result:



```
Visual cryptography is a cryptographic
technique which allows visual information
(pictures, text, etc.) to be encrypted in
such a way that decryption becomes the job
of the person to decrypt via sight reading.

One of the best-known techniqueshas been
credited to Moni Naor and Adi Shamir, who
developed it in 1994.[1] They demonstrated
a visual secret sharing scheme, where an
image was broken up into n shares so that
only someone with all n shares could decrypt
the image, while any n - 1 shares revealed
no information about the original image.

Your flag:
VolgaCTF{Classic_secret_sharing_scheme}
```

out

Flag is: VolgaCTF{Classic_secret_sharing_scheme}.

Note: *VC* is for *Visual Cryptography*

Viewed using Just Read