Challenge Name: 13

Category: Cryptography

AUTHOR: ALEX FULTON/DANIEL TUNITIS

Description

Cryptography can be easy, do you know what ROT13 is? cvpbPGS{abg_gbb_onq_bs_n_ceboyrz}

Hints 1: This can be solved online if you don't want to do it by hand!

https://play.picoctf.org/practice/challenge/62?category=2&page=1

Learning outcome : Encryption methods

*ROT-13 is one of the **simple letter substitution cipher** that replaces a letter with the 13th letter after it in the alphabet.*

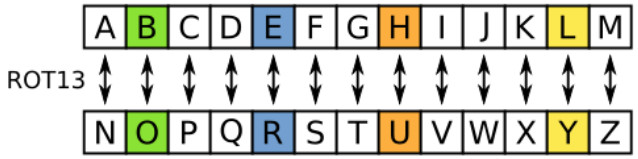
Solution

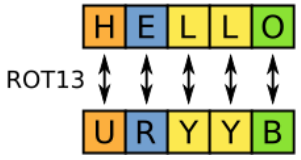
1. In Linux, type the command below:

```
echo cvpbPGS{abg_gbb_onq_bs_n_ceboyrz} | rot13
```

2. Or, go to https://gchq.github.io/CyberChef/ and use the ROT-13 as Recipe. Paste the ciphertext to the input

3. Or, manually





The answer is **picoCTF{not_too_bad_of_a_problem}**

https://blog.kuhi.to/picoctf_2019_crypto_writeup#13

挑戰名稱: 13

種類: Cryptography

作者: ALEX FULTON/DANIEL TUNITIS

描述

密碼學其實很簡單，您知道什麼是ROT13嗎？

cvpbPGS{abg_gbb_onq_bs_n_ceboyrz}

提示 1: 如果你不想用人手做，可以在網上找到解決方法！

https://play.picoctf.org/practice/challenge/62?category=2&page=1

可以學習到：加密方式

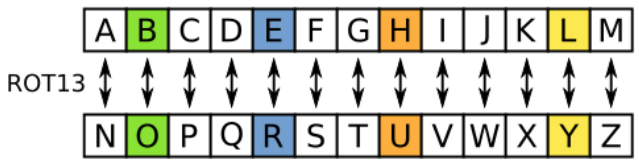
*ROT-13 是其中一種**簡單的字母替換密碼法**，你可以將字母與第 13 個字符替換。*

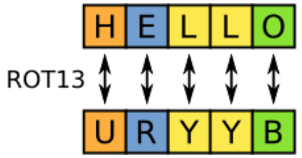
解題（3 種不同方法）

1. 在 Linux 系統中，可以打以下指令:

```
echo cvpbPGS{abg_gbb_onq_bs_n_ceboyrz} | rot13
```

2. 或到 https://gchq.github.io/CyberChef/ 並選擇 ROT-13。貼上已加密的信息即可。
3. 或人手解密





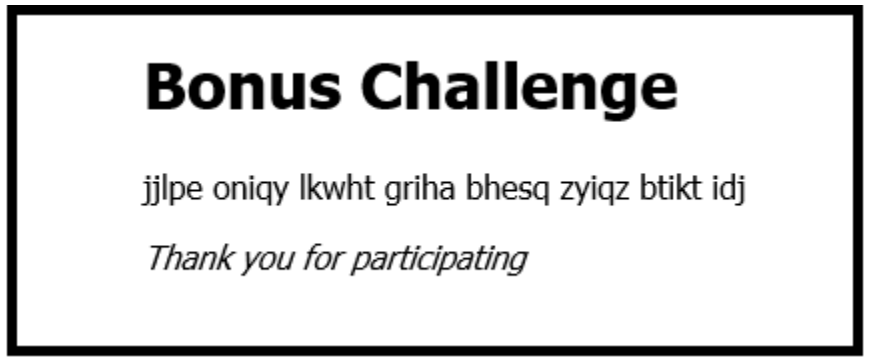
所得的旗幟是：
picoCTF{not_too_bad_of_a_problem}

https://blog.kuhi.to/picoctf_2019_crypto_writeup#13

Challenge Name: Breaking the Code - Bonus

Category: Cryptography

AUTHOR: FIRST



Description

Can you find the flag?

*(The website look and feel, please refer to the photo above)

Hints 1: Look at the HTML comments.

Hints 2: Headers: Date / Rotors / Ring Settings / Plugboard / Initial Rotor Positions

Hint 3: The message was sent before the 20th day

Learning outcome : File format, Enigma Cipher

Some file may not be open successfully caused by format changed incidentally

Solution

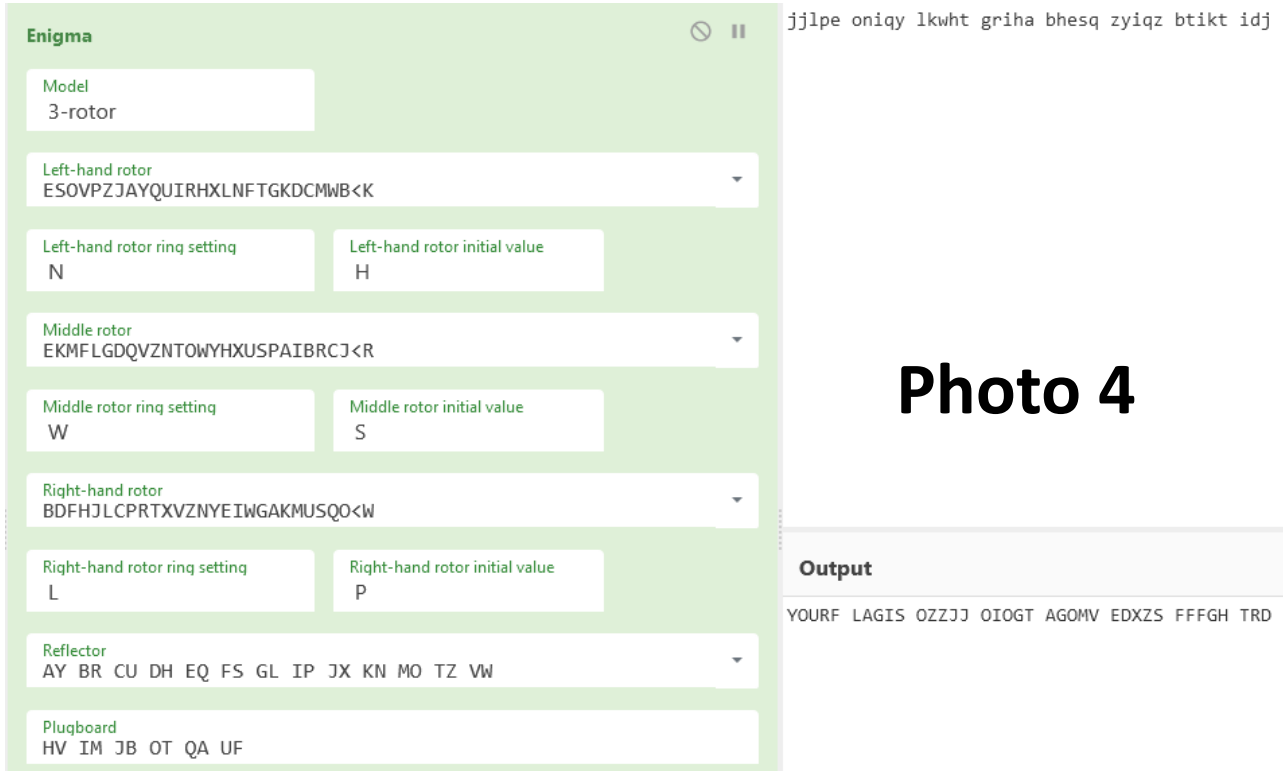
1. **Review** the source code of the website (photo 1)
2. Use **Base64** to decrypt it and get a png information (photo 2)
3. Save the output and **change** to png **file format** (photo 3)
4. **Analysis** the photo, **search** in Google image, and you should get hints and knowing it is **Enigma Cipher**
5. Follow the hints, use the **18**th and decrypt the flag by tool (photo 4)
6. The answer is **FIRSTCTF{OZZJJ OIOGT AGOMV EDXZS FFFGH TRD}**

```
<h1>Bonus Challenge</h1>
<p>jjlpe oniqy lkwht griha bhesq zyiqz btikt idj</p>

<p><em>Thank you for participating</em></p>
</body>
</html>

<!-- Bonus
iVBORw0KGgoAAAANSUhEUgAAAaAAAADcCAYAAAA2oXVXAAAABmJLR0QA/wD/AP+gvaeTAAAACXBI
WXMAAAsTAAALEwEAmpwYAAAAB3RJTUUH5AUbDSMmaoXNFQAAAB1pVFh0Q29tbWVudAAAAAAAQ3Jl
```

Photo 1



jjlpe oniqy lkwht griha bhesq zyiqz btikt idj

Output

YOURF LAGIS OZZJJ OIOGT AGOMV EDXZS FFFGH TRD

Photo 4

```
388TeulZVNWSJEm46YqX8LSPyfe88g/fz8N++FWGJ5/KsX3L4Bz/fF
IbSvTFe47v95Ked8Ut4vX/jamRwbFdE3/PnLeMYnAH6LP3vjv/Ci37
+xrHXfQ3/+f3nPIcvvnWh+H+4WM86tKb5X973gX84FEHeNV5l8f36p
3v1m4cABF1xyCS84RpPObuZlvymfgwvfewH6og8Ib44Hcsknz+OMPT
```

Output

.PNG

.

...

IHDR... ...Ü.....6¡uW....bKGD.ÿ.ÿ.ÿ ½§.... pHYs..
#&j.Í.....iTXtComment.....Created with GIMPd.e... .IDA
...¥C...)R¤£.Ð..

Photo 2

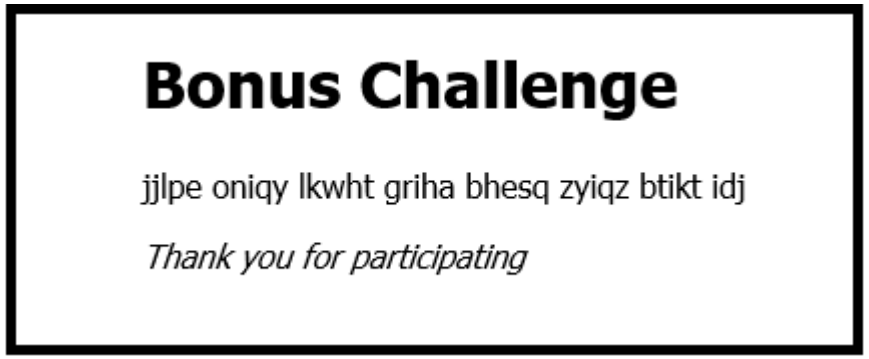
24	V III I	UCO	GC JU KE MF OD XY	BDT
23	II V IV	RWQ	BN FK OS PW TA ZE	IYM
22	IV II I	TRK	BN DU JI OK TF XC	SFX
21	II V III	CTZ	AF BK GJ VQ XH YT	TQO
20	I V III	XOM	BX IS LY NF QO WA	DKV
19	IV V II	LDQ	CR FO LI NM PD XH	IAH
18	IV I III	NWL	HV IM JB OT QA UF	HSP
17	II IV III	HFZ	FE IB OQ VC YW ZM	GPZ
16	II I IV	UBJ	CO GV IH KD ML RB	PJU
15	I II IV	BCG	ES GD IZ JF LN YA	KFQ
14	II V IV	EAP	BT CQ NE PK VY ZL	CCH

Photo 3

挑戰名稱: Breaking the Code - Bonus

類別: Cryptography

作者: FIRST



描述

你能找到旗幟嗎？

*（網站的樣式，請參閱上面的照片）

提示 1: 請檢示網頁源始碼中的評論部份

提示 2: Headers: Date / Rotors / Ring Settings / Plugboard / Initial Rotor Positions

提示 3: 信息是在第 20日前發出

可以學習到 : 文件格式 及 恩尼格瑪密碼

有些文件可能因文件格式被錯誤地修改而不能開啟

HKCERT

解題

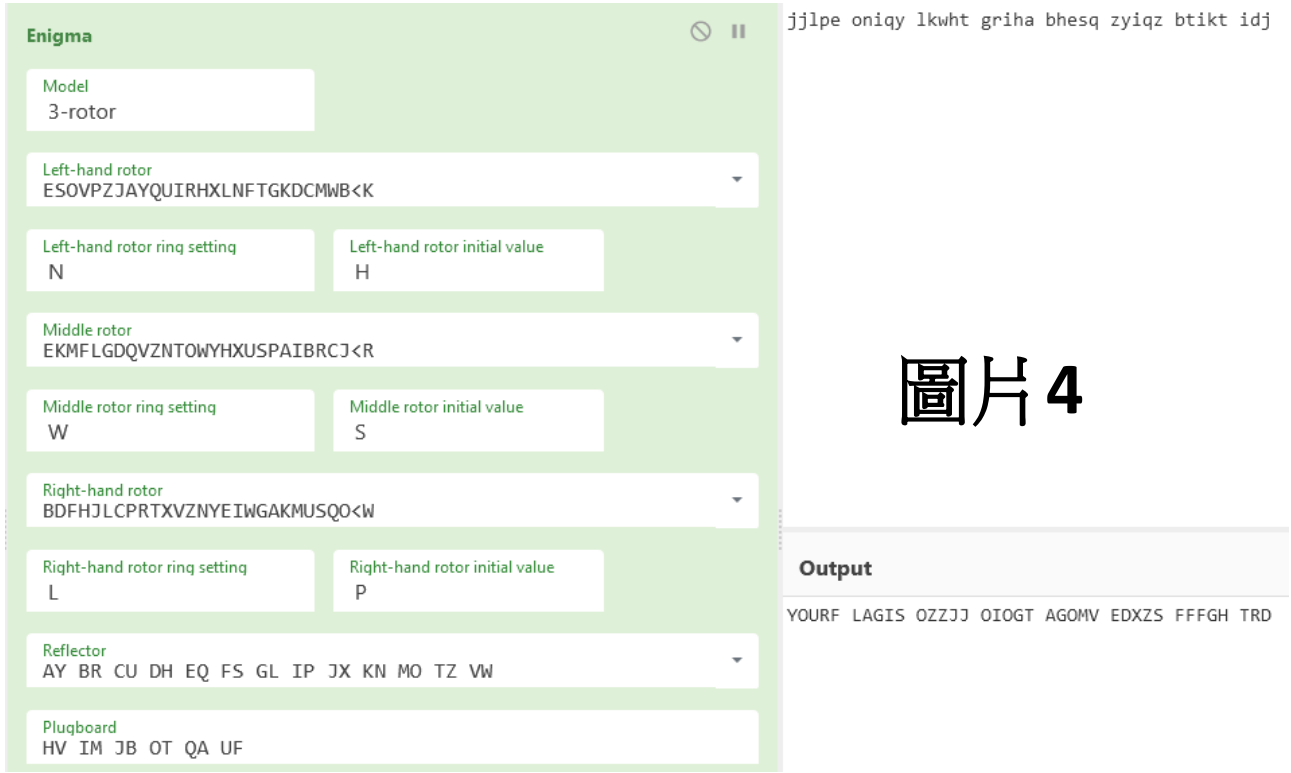
1. **檢示**網頁的源始碼 (圖片 1)
2. 使用 **Base64** 解密，並得到 png 資訊 (圖片 2)
3. **儲存**資料為**圖片 格式** (圖片 3)
4. **分析**圖片，並在 Google 中 **搜尋**，你應該可以得到一些提示並知道它**是恩尼格瑪密碼**
5. 跟據提示，用第 18 行的資料透過工具解密旗幟 (圖片 4)
6. 所得的旗幟是：“**FIRSTCTF{OZZJJ OIOGT AGOMV EDXZS FFFGH TRD}**”

```
<h1>Bonus Challenge</h1>
<p>jjlpe oniqy lkwht griha bhesq zyiqz btikt idj</p>

<p><em>Thank you for participating</em></p>
</body>
</html>

<!-- Bonus
iVBORw0KGgoAAAANSUhEUgAAAaAAAADcCAYAAAA2oXVXAAAABmJLR0QA/wD/AP+gvaeTAAAACXBI
WXMAAAsTAAALEwEAmpwYAAAAB3RJTUUH5AUbDSMmaoXNFQAAAB1pVFh0Q29tbWVudAAAAAAAQ3Jl
```

圖片 1




```
jjlpe oniqy lkwht griha bhesq zyiqz btikt idj
```

圖片 4

Output

```
YOURF LAGIS OZZJJ OIOGT AGOMV EDXZS FFFGH TRD
```

```
51JYcyoepHRwnmVT03c9C1+CPyD/6Te4/0uV/E8/3as/8MecT/+UtV
388TeulZVNWSJEm46YqX8LSPyfe88g/fz8N++FWGJ5/KsX3L4Bz/fF
IbSvTFe47v95Ked8Ut4vX/jamRwbFdE3/PnLeMYnAH6LP3vjv/Ci37
+xrHXfQ3/+f3nPIcvvnWh+H+4WM86tKb5X973gX84FEHeNV5l8f36p
3v1m4cABF1xyCS84RpPObuZlvymfgwvfewH6og8Ib44Hcsknz+OMPT
RQcHYNdw/ecv4tzL/v+/33e9kR+84aN8FYDf5kvffhInhAG8FFrH4/
```

Output

```
.PNG
.
...
IHDR... ...Ü.....6¡uW....bKGD.ÿ.ÿ.ÿ ½§....      pHYs..
#&j.Í.....iTXtComment.....Created with GIMPd.e... .IDA
...¥C...)R¤£.Ð..
```

圖片 2

24	V III I	UCO	GC JU KE MF OD XY	BDT
23	II V IV	RWQ	BN FK OS PW TA ZE	IYM
22	IV II I	TRK	BN DU JI OK TF XC	SFX
21	II V III	CTZ	AF BK GJ VQ XH YT	TQO
20	I V III	XOM	BX IS LY NF QO WA	DKV
19	IV V II	LDQ	CR FO LI NM PD XH	IAH
18	IV I III	NWL	HV IM JB OT QA UF	HSP
17	II IV III	HFZ	FE IB OQ VC YW ZM	GPZ
16	II I IV	UBJ	CO GV IH KD ML RB	PJU
15	I II IV	BCG	ES GD IZ JF LN YA	KFQ
14	II V IV	EAP	BT CQ NE PK VY ZL	CCH

圖片 3