



OLD CRYPTOGRAM

[Publish Date]

European Cyber Security Challenge 2018
London, United Kingdom

1. Initial Write-Up

Description:

You have found an old ciphertext, where you know that the plaintext discusses a biblical subject. You just finished your first classes in the topics of cryptography. Therefore, it's time to test yourself.

Make use of the new skills and try to find out what is in the back of the cryptogram. You will know if the decryption is good if you get the correct SHA- digest of the text, in hex (the flag). The old cryptogram is:

Axeeg ck vs rvmks fskhcjz enxds ck cj hvs ksdfsh mi hvs Bmfq, xjq ajqsf hvs kvxqs mi hvs rcjzk mi hvs lmkh Aczv.

Hvm kxgk mi hvs Bmfq, As ck yg kxis enxds xjq yg hmrsf mi khfsjzhv: vs ck yg Jmq, cj rvmy ck yg vmes.

As rcnn hxts gma mah mi hvs ucfq jsh, xjq tsse gma kxis ifmy rxkhcjz qcksxks.

Nma rcnn us dmwsfsq ug vck isxhvsfk; ajqsf vck rcjzk gma rcnn us kxis: vck zmmq ixchv rcnn us gmaf kxnwxhcmj.

Nma rcnn vxws jm isxf mi hvs swcn hviczjz mi hvs jczvh, mf mi hvs xffmr cj inczvh ug qxg,

Lf mi hvs qcksxks rvcdv hxtsk ysj cj hvs qxft, mf mi hvs qskhfadhcmj rvcdv yxtsk rxkhs rvsj hvs kaj ck vczv.

Nma rcnn kss x hvmaxjq ixnncjz ug gmaf kcqs, xjq hsj hvmaxjq xh gmaf fczvh vxjq; uah ch rcnn jmh dmys jsxf gma.

Ljng rchv gmaf sgsk rcnn gma kss hvs fsrfq mi hvs swcn-qmsfk.

Zsdxaks gma vxws kxcq, M xy cj hvs vxjq mi hvs Bmfq, hvs lmkh Aczv ck yg kxis fskhcjz-enxds;

Fm swcn rcnn dmys mj gma, xjq jm qcksxks rcnn dmys jsxf gmaf hsjh.

Wmf vs rcnn zcws gma cjhm hvs dxfs mi vck xjzsnk hm tsse gma rvsfswsf gma zm.

Mj hvscf vxjq hvsg rcnn tsse gma ae, km hvxh gmaf immh yxg jmh us dfakvsq xzxcjkh x khmjs.

Nma rcnn eah gmaf immh mj hvs ncmj xjq hvs kjxts; hvs gmajz ncmj xjq hvs zfsxh kjxts rcnn us dfakvsq ajqsf gmaf issh.

Zsdxaks vs vxk zcwsj ys vck nmws, M rcnn hxts vcy mah mi qxjzsf: M rcnn eah vcy cj x enxds mi vmjmaf, usdxaks vs vxk tseh yg jxys cj vck vsxfh.

Hvsj vck dfg dmysk ae hm ys, M rcnn zcws vcy xj xjkrzf: M rcnn us rchv vcy cj hfmauns;

M rcnn yxts vcy ifss ifmy qxjzsf xjq zcws vcy vmjmaf. Hchv nmjz ncis rcnn vs us fsrfqsf; xjq M rcnn nsh vcy kss yg kxnwxhcmj.

2. Challenge specifications

- Category: Crypto
- Difficulty : Easy

3. Tools needed

Description:

Tools needed for the solution of the challenge:

- General Linux tools

4. Artifacts provided

List of artifacts provided with checksums.

File name	Checksums
sub_plaintext	c8d3249a64b5d14ee86616833f917a58
sub_key	ed9b0713ccf4d773f4891633c5e5656c