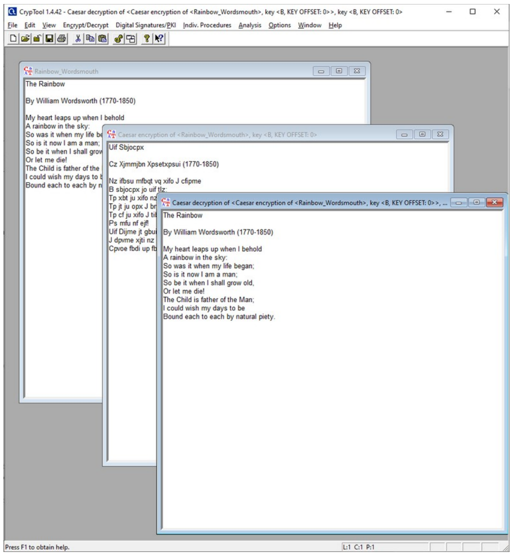
Lab 4 - Cryptography

- This is a lab assignment, and worth 5 points.
- The due date is midnight on the day it is posted. It will be graded as pass/fail (5 or 0 points). Submit this outcome file.

Answer the following questions.

1. Were you able to crack the text encrypted with Caesar/Rot-13 using Analysis > Symmetric Encryption (classic)? (Y / N)
   Yes I was able to crack the text encryption.



CrypTool 1.4.42 - Caesar decryption of <Caesar encryption of <Rainbow_Wordsmouth>, key <B, KEY OFFSET: 0>>, key <B, KEY OFFSET: 0>

File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help

Rainbow_Wordsmouth

The Rainbow

By William Wordsworth (1770-1850)

My heart leaps up when I behold
A rainbow in the sky:
So was it when my life be
So is it now I am a man;
So be it when I shall grow
Or let me die!
The Child is father of the
I could wish my days to b
Bound each to each by n

Caesar encryption of <Rainbow_Wordsmouth>, key <B, KEY OFFSET: 0>

Uif Sbjocpx

Cz Xjmmjbn Xpsetxpsui (1770-1850)

Nz ifbsu mfbqt vq xifo J cfipme
B sbjocpx jo uif tlz:
Tp xbt ju xifo nz
Tp jt ju opx J br
Tp cf ju xifo J tit
Ps mfu nf ejf!
Uif Dijme jt gbui
J dpvme xjti nz
Cpvoe fbdi up fb

Caesar decryption of <Caesar encryption of <Rainbow_Wordsmouth>, key <B, KEY OFFSET: 0>>, ...

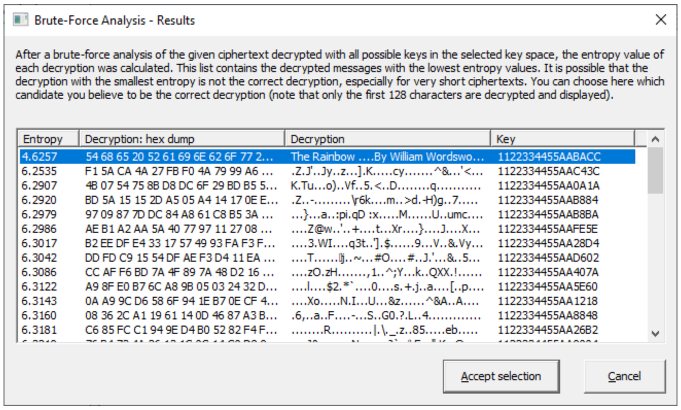
The Rainbow

By William Wordsworth (1770-1850)

My heart leaps up when I behold
A rainbow in the sky:
So was it when my life began;
So is it now I am a man;
So be it when I shall grow old,
Or let me die!
The Child is father of the Man;
I could wish my days to be
Bound each to each by natural piety.

Press F1 to obtain help. L:1 C:1 P:1

2. How long did it take to brute force the key for the text encrypted with DES (ECB) when the last four hex codes of the key are not known?
   It was instantaneous using the Analysis option and brute forcing the last four digits.

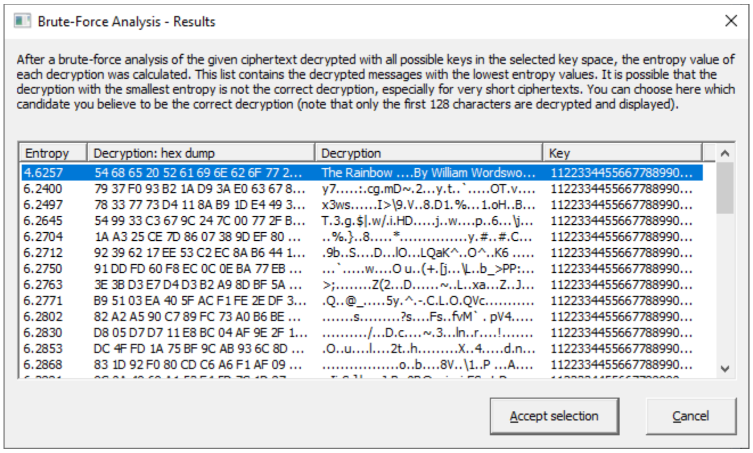


Brute-Force Analysis - Results

After a brute-force analysis of the given ciphertext decrypted with all possible keys in the selected key space, the entropy value of each decryption was calculated. This list contains the decrypted messages with the lowest entropy values. It is possible that the decryption with the smallest entropy is not the correct decryption, especially for very short ciphertexts. You can choose here which candidate you believe to be the correct decryption (note that only the first 128 characters are decrypted and displayed).

Entropy	Decryption: hex dump	Decryption	Key
4.6257	54 68 65 20 52 61 69 6E 62 6F 77 2...	The Rainbow ....By William Wordswo...	1122334455AABACC
6.2535	F1 5A CA 4A 27 FB F0 4A 79 99 A6 ...	.Z.J'..Jy..z...].K.....cy.......^&...'<...	1122334455AAC43C
6.2907	4B 07 54 75 8B D8 DC 6F 29 BD B5 5...	K.Tu...o)..Vf..5.<..D........q..........	1122334455AA0A1A
6.2920	BD 5A 15 15 2D A5 05 A4 14 17 0E E...	.Z..-.........\r6k....m..>d.-H)g..7.....	1122334455AAB884
6.2979	97 09 87 7D DC 84 A8 61 C8 B5 3A ...	...}...a..:pi.qD :x.....M......U..umc....	1122334455AAB8BA
6.2986	AE B1 A2 AA 5A 40 77 97 11 27 08 ...	....Z@w..'..+....t...Xr....}....J....X...	1122334455AAFE5E
6.3017	B2 EE DF E4 33 17 57 49 93 FA F3 F...	....3.WI....q3t..'].$......9...V..&.Vy...	1122334455AA28D4
6.3042	DD FD C9 15 54 DF AE F3 D4 11 EA ...	....T.......ĳ..~...#O....#..J.'...&..5...	1122334455AAD602
6.3086	CC AF F6 BD 7A 4F 89 7A 48 D2 16 ...	....zO.zH.......,1..^;Y...k..QXX.!......	1122334455AA407A
6.3122	A9 8F E0 B7 6C A8 9B 05 03 24 32 D...	....l....$2.*`....0....s.+.j..a....[..p....	1122334455AA5E60
6.3143	0A A9 9C D6 58 6F 94 1E B7 0E CF 4...	....Xo.....N.I...U...&z......^&A..A....	1122334455AA1218
6.3160	08 36 2C A1 19 61 14 0D 46 87 A3 B...	.6,..a..F....-...S..G0.?.L..4............	1122334455AA8848
6.3181	C6 85 FC C1 94 9E D4 B0 52 82 F4 F...	........R..........|.\._.z..85.....eb.....	1122334455AA26B2

3. How long did it take to brute force the key for the text encrypted with Reijndael (AES) when the last four hex codes of the key are not known?
   It would still take more time than the previous DES one since there are more keys in it but it was still instant.



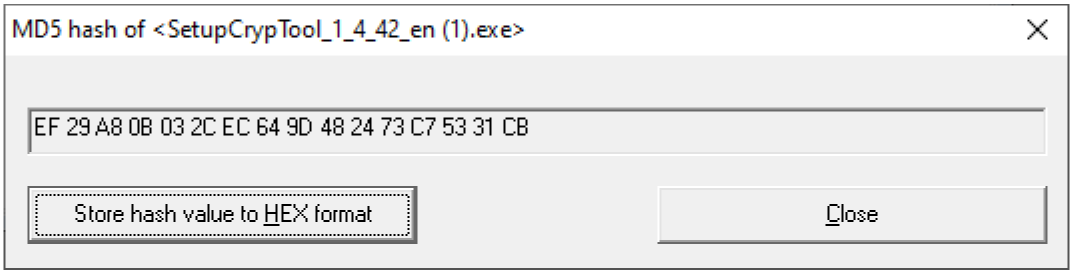
Brute-Force Analysis - Results

After a brute-force analysis of the given ciphertext decrypted with all possible keys in the selected key space, the entropy value of each decryption was calculated. This list contains the decrypted messages with the lowest entropy values. It is possible that the decryption with the smallest entropy is not the correct decryption, especially for very short ciphertexts. You can choose here which candidate you believe to be the correct decryption (note that only the first 128 characters are decrypted and displayed).

<table>
<tr><th>Entropy</th><th>Decryption: hex dump</th><th>Decryption</th><th>Key</th></tr>
<tr><td>4.6257</td><td>54 68 65 20 52 61 69 6E 62 6F 77 2...</td><td>The Rainbow ....By William Wordswo...</td><td>1122334455667788990...</td></tr>
<tr><td>6.2400</td><td>79 37 F0 93 B2 1A D9 3A E0 63 67 8...</td><td>y7.....:.cg.mD~.2...y.t..`.....OT.v....</td><td>1122334455667788990...</td></tr>
<tr><td>6.2497</td><td>78 33 77 73 D4 11 8A B9 1D E4 49 3...</td><td>x3ws......I>\9.V..8.D1.%...1.oH..B...</td><td>1122334455667788990...</td></tr>
<tr><td>6.2645</td><td>54 99 33 C3 67 9C 24 7C 00 77 2F B...</td><td>T.3.g.$|.w/.i.HD.....j..w....p..6...\j...</td><td>1122334455667788990...</td></tr>
<tr><td>6.2704</td><td>1A A3 25 CE 7D 86 07 38 9D EF 80 ...</td><td>..%.}..8.....*..............y.#..#.C...</td><td>1122334455667788990...</td></tr>
<tr><td>6.2712</td><td>92 39 62 17 EE 53 C2 EC 8A B6 44 1...</td><td>.9b..S....D...lO...LQaK^..O^..K6 .....</td><td>1122334455667788990...</td></tr>
<tr><td>6.2750</td><td>91 DD FD 60 F8 EC 0C 0E BA 77 EB ...</td><td>...`.....w....O u..(+.[j...\L..b_>PP:...</td><td>1122334455667788990...</td></tr>
<tr><td>6.2763</td><td>3E 3B D3 E7 D4 D3 B2 A9 8D BF 5A ...</td><td>>;........Z(2...D......~..L..xa...Z..J...</td><td>1122334455667788990...</td></tr>
<tr><td>6.2771</td><td>B9 51 03 EA 40 5F AC F1 FE 2E DF 3...</td><td>.Q..@_.....5y.^.-.C.L.O.QVc..........</td><td>1122334455667788990...</td></tr>
<tr><td>6.2802</td><td>82 A2 A5 90 C7 89 FC 73 A0 B6 BE ...</td><td>.......s.........?s....Fs..fvM` . pV4.....</td><td>1122334455667788990...</td></tr>
<tr><td>6.2830</td><td>D8 05 D7 D7 11 E8 BC 04 AF 9E 2F 1...</td><td>........./...D.c....~.3...ln..r....!.......</td><td>1122334455667788990...</td></tr>
<tr><td>6.2853</td><td>DC 4F FD 1A 75 BF 9C AB 93 6C 8D ...</td><td>.O..u....l....2t..h.........X..4.....d.n...</td><td>1122334455667788990...</td></tr>
<tr><td>6.2868</td><td>83 1D 92 F0 80 CD C6 A6 F1 AF 09 ...</td><td>................o..b....8V..\1..P ...A....</td><td>1122334455667788990...</td></tr>
</table>

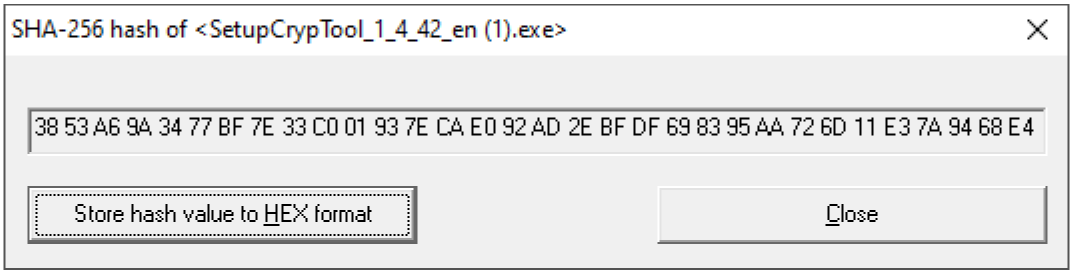
4. Were you able to verify the digital signature? (Y   /   N   )
   Yes

5. Are the hash values for CrypTool 1.4.42 (what you have calculated and the one on the cryptool.org website) the same? (Yes   /   No   )
   The SHA-256 hash is the same as on the website once you run it. But it is different if you use the MD5 hash value. SHA-256 is the same but MD5 is not.



MD5 hash of <SetupCrypTool_1_4_42_en (1).exe>

EF 29 A8 0B 03 2C EC 64 9D 48 24 73 C7 53 31 CB



SHA-256 hash of <SetupCrypTool_1_4_42_en (1).exe>

38 53 A6 9A 34 77 BF 7E 33 C0 01 93 7E CA E0 92 AD 2E BF DF 69 83 95 AA 72 6D 11 E3 7A 94 68 E4