

Forum:[Hack Forums](#)

Thread: [Help Decrypt / Bruteforce DES Ciphertext](#)

Yellow - August 15, 2019, 7:28 am

I've been given ciphertext which has been encrypted with DES.

Ciphertext:

Code 0x ce 12 6d 2d df 2d 1e 64

I have also been given a hint on what the final section of the DES encrypt key is:

Code 0x ZZ ZZ ZZ ZZ ZZ e5 f6 66

Where ZZ are the components in which I need to calculate / find out for the correct key.

I am also told that the plaintext is all capital letters (8 capital letters, 2 4 letter words with no space)

I have written a basic program in C# which attempts to decrypt the cipher and then check if the decryption is only capital letters but it seems to be relatively slow. (I used a C# DES Encrypt/Decrypt String [altered to reference my hex cipher text] using DES example from CodeProject to build my solution)[cannot post links as I do not have 50 posts]

I was wondering if anyone has a better or faster approach into helping me to acquire the correct key.

Many thanks!

AbakBarama - August 15, 2019, 9:31 am

(Aug 15, 2019 07:28 AM)Yellow Wrote: [\[CITE\]](#) I was wondering if anyone has a better or faster approach into helping me to acquire the correct key.

I suppose you'll find a lot of keys, not single key.

Full number of 8-bytes combinations: 18 446 744 073 709 551 616.

Number of combinations with capital letters only: 208 827 064 576.

Approx. 1 of 88 335 025 combinations will contain capital letters only.

5 unknown bytes from key, 7 unknown bits in each byte --> 34 359 738 368 attempts are needed.

Brutforcing all keyspace will give approx. 389 different keys with valid plaintexts.

Average speed on CPU is about 1e6..2e6 keys per sec.

Estimated time for your task will be 10-20 hours.

Yellow - August 15, 2019, 5:44 pm

(Aug 15, 2019 09:31 AM)AbakBarama Wrote: [\[CITE\]](#) I suppose you'll find a lot of keys, not single key.

Full number of 8-bytes combinations: 18 446 744 073 709 551 616.

Number of combinations with capital letters only: 208 827 064 576.

Approx. 1 of 88 335 025 combinations will contain capital letters only.

5 unknown bytes from key, 7 unknown bits in each byte --> 34 359 738 368 attempts are needed.

Brutforcing all keyspace will give approx. 389 different keys with valid plaintexts.

Average speed on CPU is about 1e6..2e6 keys per sec.

Estimated time for your task will be 10-20 hours.

I'm getting an exception thrown when I decrypt with the wrong key, so I'm using a try catch approach, with nothing inside the catch to pass this.

I believe the try catch is what's making my code operate slow as I've been running it for over 1 day.

I'm not sure how to brute force in an efficient / quick manner.

991z3r0 - August 15, 2019, 6:24 pm

(Aug 15, 2019 05:44 PM)Yellow Wrote: [\[CITE\]](#) I'm getting an exception thrown when I decrypt with the wrong key, so I'm using a try catch approach, with nothing inside the catch to pass this.

I believe the try catch is what's making my code operate slow as I've been running it for over 1 day.

I'm not sure how to brute force in an efficient / quick manner.

Split the work up into many threads, that should help with processing speed.

AbakBarama - August 16, 2019, 6:23 am

(Aug 15, 2019 05:44 PM)Yellow Wrote: [\[CITE\]](#) I'm not sure how to brute force in an efficient / quick manner.

I've tried to make bruteforcer on C#, it works 50-100 times slower then C program. I don't explain such a huge difference.

If you want to write your own C/C++ bruteforcer then you can easily find DES C sources, for example [GitHub - schwabe/polarssl: A portable, easy to use, readable and flexible SSL library \(dual-licensed\)](#)

Some valid keys and plaintexts:

00 00 B0 56 82 E5 F6 66 --> LIFOBHJU
00 B8 7E 28 8A E5 F6 66 --> NVAZLXVC
00 BC 7E 34 18 E5 F6 66 --> HRVYUICA
00 C2 EE 6E 5C E5 F6 66 --> KISSVGKM
00 EE C0 4A EC E5 F6 66 --> TBELFEAL

Estimated number of valid results is about 400.

Yellow - August 16, 2019, 9:59 pm

(Aug 16, 2019 06:23 AM)AbakBarama Wrote: [\[CITE\]](#) I've tried to make bruteforcer on C#, it works 50-100 times slower then C program. I don't explain such a huge difference.

If you want to write your own C/C++ bruteforcer then you can easily find DES C sources, for example

Some valid keys and plaintexts:

00 00 B0 56 82 E5 F6 66 --> LIFOBHJU
00 B8 7E 28 8A E5 F6 66 --> NVAZLXVC
00 BC 7E 34 18 E5 F6 66 --> HRVYUICA
00 C2 EE 6E 5C E5 F6 66 --> KISSVGKM
00 EE C0 4A EC E5 F6 66 --> TBELFEAL

Estimated number of valid results is about 400.

I've also been told that the plaintext is 2 4 letter words. Eg BLUETREE. I can't send you a PM as I don't reach the post requirements, I was wondering if you could send me your bruteforcer on C# as I've noticed you've gotten some valid results (ie could you PM me etc?)

AbakBarama - *August 17, 2019, 1:43 am*

(Aug 16, 2019 09:59 PM)Yellow Wrote: [CITE](#) could you PM me etc?
PM sent.