

Forum:[Hack Forums](#)

Thread: [help identifying type of encryption](#)

bbe24 - March 21, 2024, 11:50 am

Is anyone familiar with this style of encryption? And how I would go about decrypting it:

\$C\$537\$1\$EFzprQuXCfz0IH5eXVPQ+w==\$DD6TGnwOZ1WYKFHLKmbbvheF2S3TDdb5xNHCW2
FYnS/JQwd7KlgXwPovocMFNAYdU

kvothesplank - March 21, 2024, 12:02 pm

Looks like a hash, like PBKDF2 or something, but it might be a custom format, tried it in a few tools and couldn't get a match.

DramaKing - March 21, 2024, 12:42 pm

(Mar 21, 2024 11:50 AM)bbe24 Wrote: [\[CITE\]](#) Is anyone familiar with this style of encryption? And how I would go about decrypting it:

\$C\$537\$1\$EFzprQuXCfz0IH5eXVPQ+w==\$DD6TGnwOZ1WYKFHLKmbbvheF2S3TDdb5xNHCW2
FYnS/JQwd7KlgXwPovocMFNAYdU

How did you go about getting it?

bbe24 - March 21, 2024, 1:17 pm

(Mar 21, 2024 12:42 PM)DramaKing Wrote: [\[CITE\]](#) How did you go about getting it?

I'm using some old software to track customers in a sql database. The software company has the encryption key for it, but they went out of business and said that all customer keys were lost in a fire and they cannot provide anyone with the keys. So unless I can decrypt it, I have no way of exporting and transferring my customer list to new software. Ugh.

DramaKing - March 21, 2024, 1:47 pm

(Mar 21, 2024 01:17 PM)bbe24 Wrote: [\[CITE\]](#) I'm using some old software to track customers in a sql database. The software company has the encryption key for it, but they went out of business and said that all customer keys were lost in a fire and they cannot provide anyone with the keys. So unless I can decrypt it, I have no way of exporting and transferring my customer list to new software. Ugh.

Okay, that's the raw hash of the license key out of the SQL database. It's impossible.

Let me dumb down encryption and hashing for you. Encryption is using a key to transform plaintext into ciphertext and then using that key or the other half of a key pair for decryption. Hashes are mathematical algorithms that are designed to be one-way. The only way to 'crack' them is, essentially, by getting lucky and coming up with plaintext that matches the hash. Using Windows license keys as an example, it's 25 alphanumeric characters, which provides $\sim 8 \times 10^{25}$ possibilities.

bbe24 - March 21, 2024, 8:12 pm

(Mar 21, 2024 01:47 PM)DramaKing Wrote: [\[CITE\]](#) Okay, that's the raw hash of the license key out of the SQL database. It's impossible.

Let me dumb down encryption and hashing for you. Encryption is using a key to transform plaintext

into ciphertext and then using that key or the other half of a key pair for decryption. Hashes are mathematical algorithms that are designed to be one-way. The only way to 'crack' them is, essentially, by getting lucky and coming up with plaintext that matches the hash. Using Windows license keys as an example, it's 25 alphanumeric characters, which provides $\sim 8 \times 10^{25}$ possibilities. Thank you sir. I appreciate you sharing your knowledge with me and not making me feel stupid lol.

What if I had the hashed value, and the original value, and I could provide a few examples of each. Is there a software that can take the hashed and unhashed values, and determine the key/formula to it?

DramaKing - March 22, 2024, 6:06 am

(Mar 21, 2024 08:12 PM)bbe24 Wrote: [\[CITE\]](#) Thank you sir. I appreciate you sharing your knowledge with me and not making me feel stupid lol.

What if I had the hashed value, and the original value, and I could provide a few examples of each. Is there a software that can take the hashed and unhashed values, and determine the key/formula to it?

Afraid not. If the data was encrypted, then one could derive the encryption key from the known plaintext and ciphertext. Hashing algorithms use a series of operations, meaning that it's impossible to know what each of those operations is just by looking at the input and output.

However, if the length of the hashes differs, then they aren't any using any kind of algorithm that I've ever heard of.