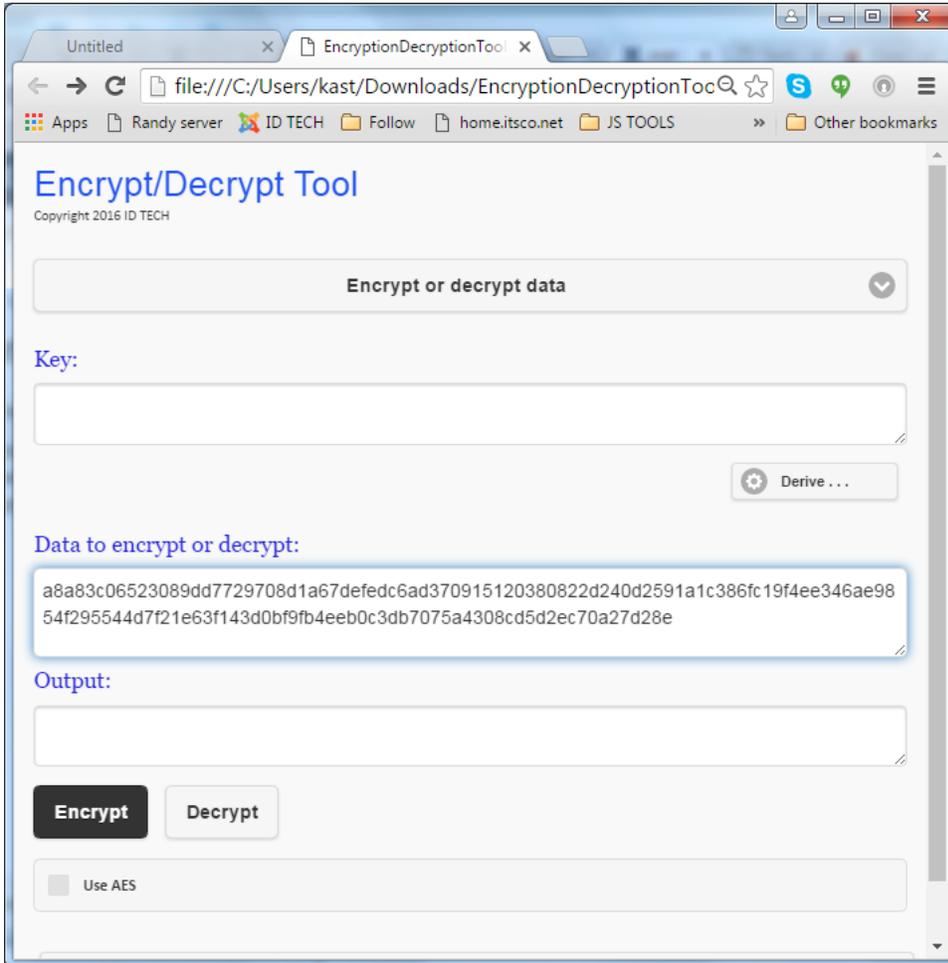


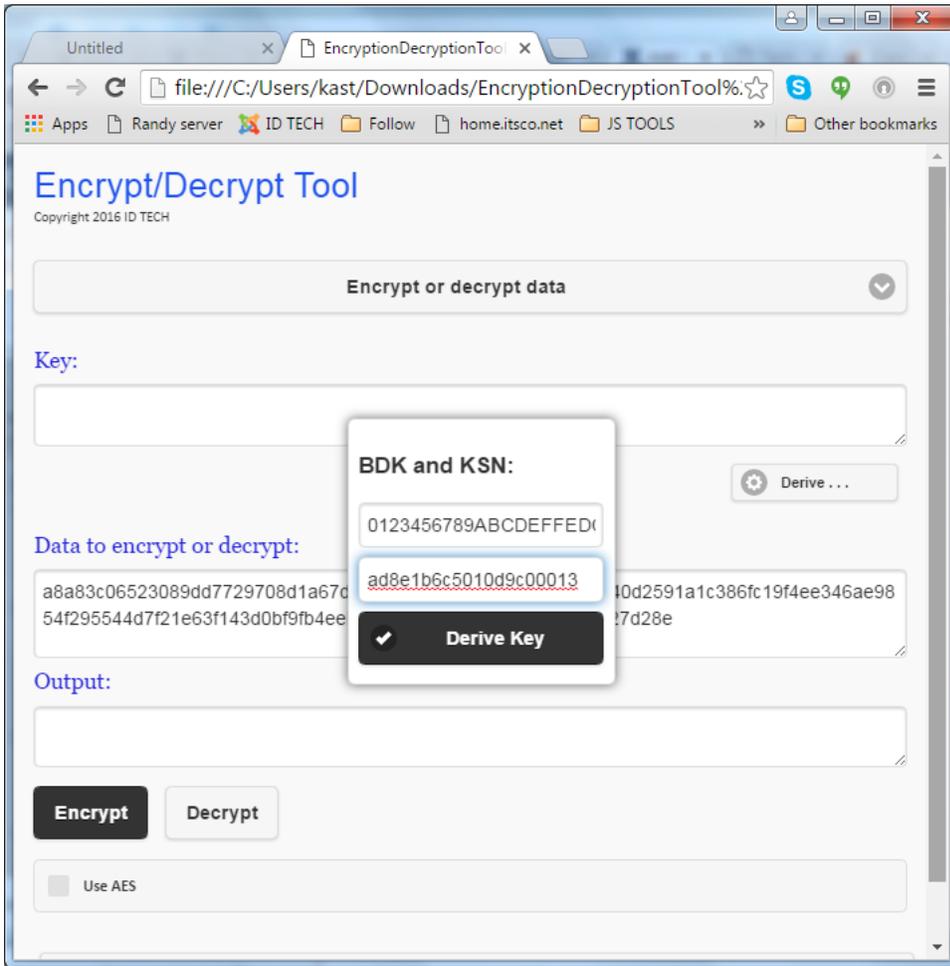
How to decrypt transaction data using test key and KSN?

This is a 60-second tutorial on how to use the Encrypt/Decrypt tool ([EncryptionDecryptionTool.html](#)) to decrypt a chunk of encrypted transaction data, such as Track 1 data or TLV data, from a card reader that does encryption.

1. First, download the [Encrypt/Decrypt tool](#) to your local machine. Save it anywhere.
2. Open the tool with your favorite web browser. It should look like the screen shot below. NOTE: If the top control says "What would you like to do?", click it and choose **Encrypt or decrypt data** from the drop-down menu.
3. Copy and paste the encrypted data (which you want to decrypt) into the **Data** field of the tool, as shown below:



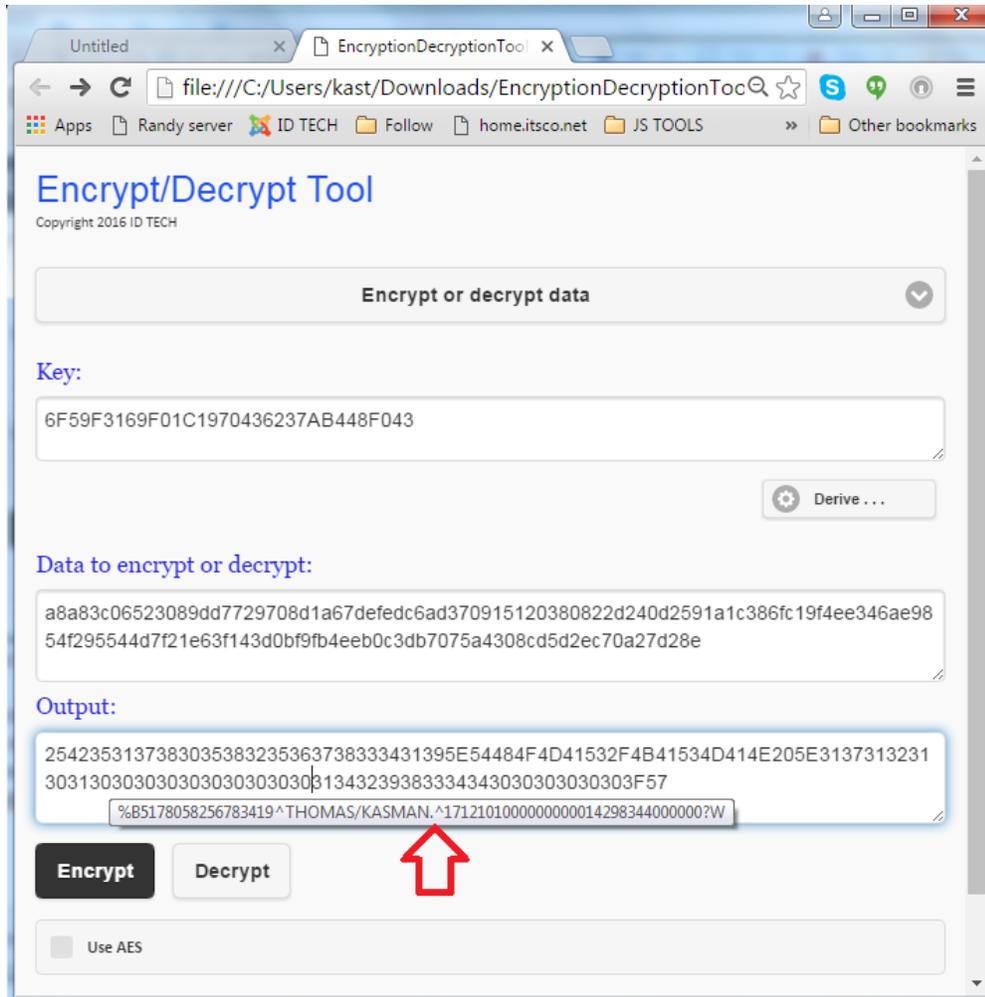
4. Click the small **Derive...** button (under the Key field, on the right; see screen shot above).
5. A small dialog will pop up. The dialog has two text fields. The top one is for the BDK. This field is prepopulated with a test key value of **0123456789ABCDEFEDCBA9876543210**. (If this is not the actual BDK you want to use, type or paste the correct value into the field.)
6. Obtain the KSN for your transaction. (It will be ten hex values.) Enter it into the second text field, as shown below:



NOTE: The hex value can be upper and lower case and may (optionally) contain spaces.

7. Click the **Derive Key** button. A key value will appear, behind the dialog, in the **Key** field of the main window.
8. To dismiss the small popup dialog, simply click into the main window.
9. If your data is AES-encrypted, click the **Use AES** checkbox at the bottom of the main window. If your data is TDES-encrypted (or you don't know), go to the next step.

Click the **Decrypt** button. A hex string will appear in the lowermost text field (the Output field). Tip: Hover your cursor over the Output field to see a tooltip containing the ASCII version of the decrypted data (see red arrow below).



Congratulations! You've decrypted TDES (or AES) transaction data using a derived DUKPT key.

See also:

- [Downloads - Home > 80128801-006-A Demo decrypt usb-HID usb-KBRS232 SecuRED V1.06.zip](#)
- [Downloads - Home > 80128801-006-A Demo decrypt usb-HID usb-KBRS232 SecuRED V1.06 SRC.zip](#)
- [Tools for Payment Device Integration: Encrypt/Decrypt Tool - ID TECH](#)
- [Downloads - Home > DukptUtility v1.0.1.0.exe](#)
- [Downloads - Home > 80110506-001-A UniMag Decryption Demo User Manual.pdf](#)
- [How to decrypt a PIN block \(tag 99\) using uDemo?](#)
- [Understanding PIN Pad Encryption/Decryption](#)
- [How to decrypt transaction data using test key and KSN?](#)
- [How can I decrypt encrypted data?](#)