Subject: Cyber Security Research Area: Security

**Credit-card encryption and decryption**

**Author’s Names:** I Kaustubh Sastry, Abhiram Molugu, K V Manohar Karthik, Dr. S. Balaji (Prof.)

**Abstract:** Credit cards are usually encrypted in order to reduce the chances of sensitive information like CVV, Passwords etc. The encryption of a credit/debit card consists of the security measures taken within the card and the encryption algorithms used in the back end of the system. Stronger the algorithm, more secure the encryption algorithm, more secure is our credit/debit card. When the credit card owner swipes the card to the machine, our sensitive information such as account number, CVV etc. are scrambled using some encryption algorithms like RSA. RSA has stood nearly 40 years of attacks, making it the choice for internet transactions and card transactions. This information is gathered by the machine using the magnetic strip at the back of the card. The magnetic strip fetches the information to the scanner only when the encryption keys match. This ensures stronger security to the credit cards. There are other types of cards which have an embedded electronic chip in them which may make it even harder to steal information. This type of card is known as a smart card.

The process of decryption is exactly the reverse process of encryption. You can use any of the number of existing open-source implementations of AES or TDES mode, which contains a default initial vector of all zero bytes. Suppose we are having the exact 16-byte decryption key, the process of decryption is easy. Then comes the actual tricky part which is the key derivation. The basic things we need to remember is the key used in the encryption process and the algorithm used. Thus, the decryption is done using the key. These days, each and every credit-card data is encrypted using a key, that is obtained using a special key-management scheme called Derived Unique Key Per Transaction (DUKPT). There is one thing to understand that in the DUKPT world, every transaction has its own key. Replay-attacks are impossible since the key used cannot be used again for other transactions.