APPENDIX T
KERBEROS ENCRYPTION TECHNIQUES

William Stallings

Supplement to
Cryptography and Network Security, Sixth Edition
Prentice Hall 2013
ISBN: 0133354695
http://williamstallings.com/Cryptography

Kerberos includes an encryption library that supports various encryption-related operations. These were included in the Kerberos version 5 specification and are common in commercial implementations. In February 2005, IETF issued RFCs 3961 and 3962, which expand the options of cryptographic techniques. In this appendix, we describe the original techniques.

T.1 PASSWORD-TO-KEY TRANSFORMATION

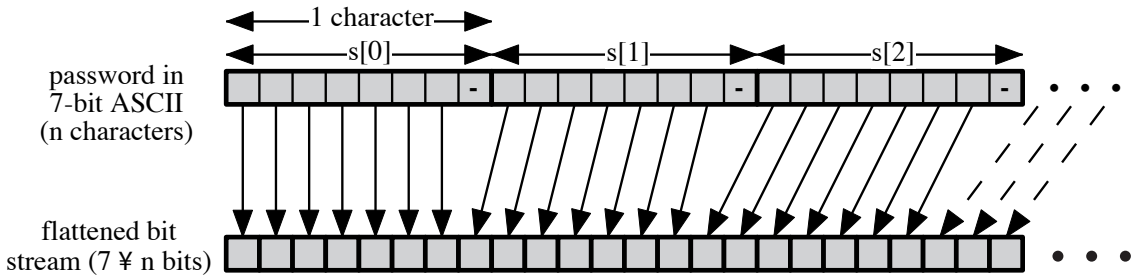
In Kerberos, passwords are limited to the use of the characters that can be represented in a 7-bit ASCII format. This password, of arbitrary length, is converted into an encryption key that is stored in the Kerberos database. Figure T.1 illustrates the procedure.

First, the character string, s, is packed into a bit string, b, such that the first character is stored in the first 7 bits, the second character in the second 7 bits, and so on. This can be expressed as

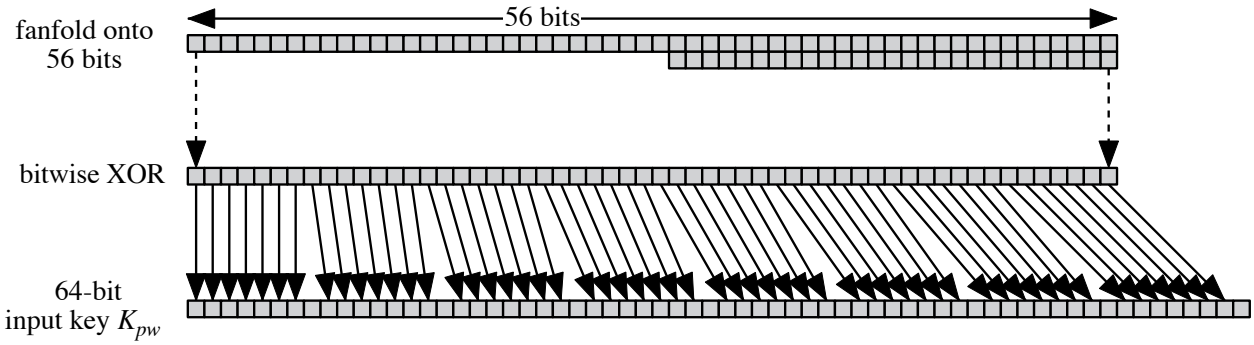
$$
\begin{aligned}
&b[0] = \text{bit 0 of } s[0] \\
&\ldots \\
&b[6] = \text{bit 6 of } s[0] \\
&b[7] = \text{bit 0 of } s[1] \\
&\ldots \\
&b[7i + m] = \text{bit } m \text{ of } s[i] \qquad 0 \leq m \leq 6
\end{aligned}
$$

Next, the bit string is compacted to 56 bits by aligning the bits in "fanfold" fashion and performing a bitwise XOR. For example, if the bit string is of length 59, then

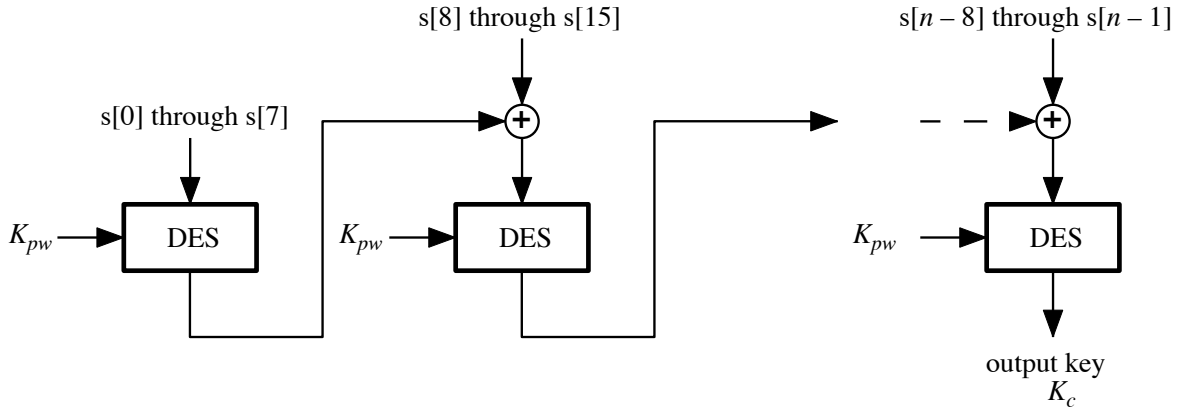
$$
\begin{aligned}
b[55] &= b[55] \oplus b[56] \\
b[54] &= b[54] \oplus b[57] \\
b[53] &= b[53] \oplus b[58]
\end{aligned}
$$



(a) Convert password to bit stream



(b) Convert bit stream to input key



(c) Generate DES CBC checksum of password

Figure T.1 Generation of Encryption Key from Password

This creates a 56-bit DES key. To conform to the expected 64-bit key format, the string is treated as a sequence of eight 7-bit blocks and is mapped into eight 8-bit blocks to form an input key K_{pw}.

Finally, the original password is encrypted using the cipher block chaining (CBC) mode of DES with key K_{pw}. The last 64-bit block returned from this process, known as the CBC checksum, is the output key associated with this password.

The entire algorithm can be viewed as a hash function that maps an arbitrary password into a 64-bit hash code.

T.2 PROPAGATING CIPHER BLOCK CHAINING MODE

Recall from Chapter 6 that, in the CBC mode of DES, the input to the DES algorithm at each stage consists of the XOR of the current plaintext block and the preceding ciphertext block with the same key used for each block (Figure 6.4). The advantage of this mode over the electronic codebook (ECB) mode, in which each plaintext block is independently encrypted, is this: With CBC, the same plaintext block produces different ciphertext blocks if repeated.

CBC has the property that if an error occurs in transmission of ciphertext block C_I, then this error propagates to the recovered plaintext blocks P_I and P_{I+1}.

Version 4 of Kerberos uses an extension to CBC called the propagating CBC (PCBC) mode [MEYE82]. This mode has the property that an error in one ciphertext block is propagated to all subsequent decrypted blocks of the message, rendering each block useless. Thus, data encryption and integrity are combined in one operation. (For an exception, see Problem 15.6).

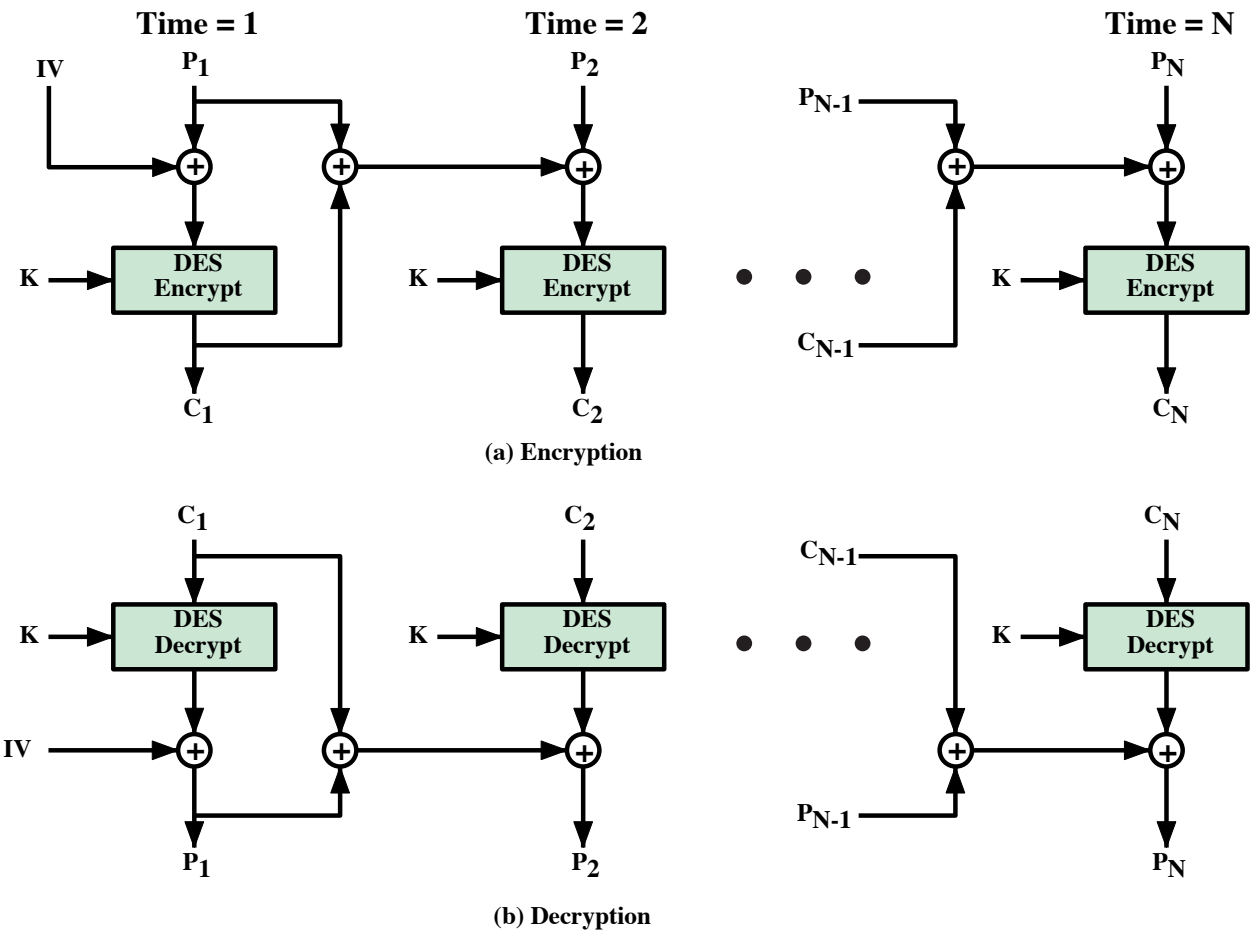


Figure T.2 Propagating Cipher Block Chaining (PCBC) Mode

PCBC is illustrated in Figure T.2. In this scheme, the input to the encryption algorithm is the XOR of the current plaintext block, the preceding cipher text block, and the preceding plaintext block:

$$C_n = E(K, [C_{n-1} \oplus P_{n-1} \oplus P_n])$$

On decryption, each ciphertext block is passed through the decryption algorithm. Then the output is XORed with the preceding ciphertext block and the preceding plaintext block. We can demonstrate that this scheme works, as follows

$$D(K, C_n) = D(K, E(K, [C_{n-1} \oplus P_{n-1} \oplus P_n]))$$

$$D(K, C_n) = C_{n-1} \oplus P_{n-1} \oplus P_n$$

$$C_{n-1} \oplus P_{n-1} \oplus D(K, C_n) = P_n$$