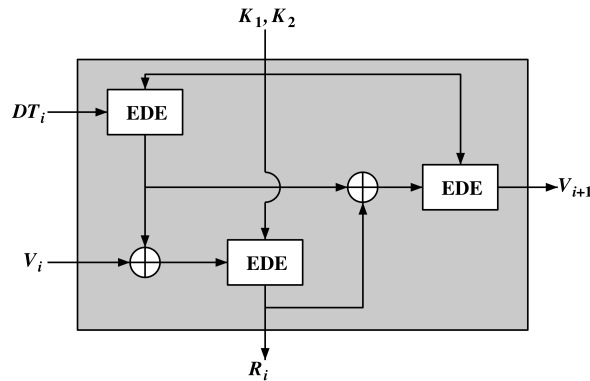


1. (20pts) Consider the diagram of the ANSI X9.17 PRNG below:



The value  $R_i$  of the generated pseudo-random value can be written as:

$$R_i = EDE(K_1||K_2; V_i \oplus EDE(K_1||K_2; DT_i)),$$

where  $EDE$  stands for 3-DES with two keys.

(10pts) Simplify (as much as possible) the above expression if  $K_1 = K_2$ .

$$R_i = DES(K_1; V_i \oplus DES(K_1; DT_i)).$$

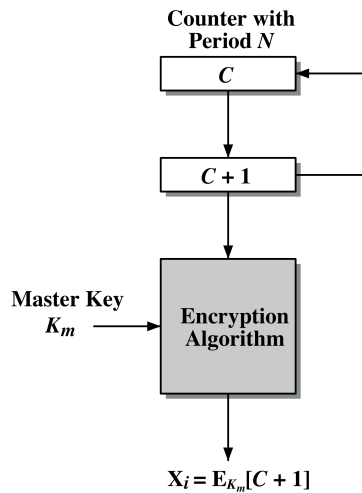
(10pts) Reading the diagram, write a similar expression for  $V_{i+1}$  in terms of  $DT_i$  and  $R_i$ .

$$V_{i+1} = EDE(K_1||K_2; R_i \oplus EDE(K_1||K_2; DT_i)).$$

2. (15pts) Answer TRUE or FALSE to each of the questions below?

- A pseudo-random number generator may pass statistical randomness tests and not be unpredictable, hence not useful in cryptography. TRUE \*\*\*\*
- For any cipher, triple encryption results in higher security than single encryption. FALSE \*\*\*
- For any cipher, double encryption does not result in much increased security due to the meet-in-the-middle attack. TRUE \*\*\*\*
- The meet-in-the-middle attack on double encryption is a given plaintext attack. TRUE \*\*\*\*
- The meet-in-the-middle attack on triple encryption is a chosen-plaintext attack. TRUE \*\*\*\*

3. (15pts) Draw a diagram of Cyclic Encryption being used to generate pseudo-random numbers.



4. (15 pts) Suppose that someone suggest the following way to confirm that the two of you are both of you are in possession of the same secret key. You create a random bit string the length of the key, XOR it with the key, and send the result over the channel. Your partner XORs the incoming block with the key (which should be the same as your key) and sends it back. You check, and if what you receive is your original random string, you have verified that your partner has the same secret key, yet neither of you has ever transmitted the key. Is there a flaw in this scheme? Explain.

Solution: The sender sends  $K \oplus R$ , where  $K$  is the key and  $R$  the random value. The receiver confirms by sending  $R$ . A passive eavesdropper who collects both  $K \oplus R$  and  $R$  is able to recover  $K = (K \oplus R) \oplus R$ , the secret key. Therefore the scheme is flawed.

5. (15 pts) List three ways in which *session keys* can be distributed.

Solution: Session keys can be send encrypted under the master key, they can be derived from the master key using a pseudo-random number generator, and they can be distributed using a key distribution center.

6. (36 pts) Answer with TRUE or FALSE.

- The Blowfish S-Boxes are key-dependent. TRUE \*\*\*\*.
- Even if the Blowfish key is all zeros, the  $P$ -array will have non-zero values. TRUE \*\*\*\*.
- Even if the Skipjack key is all zeros, the key schedule will have non-zero values. FALSE \*\*\*.
- The Skipjack S-Boxes are key dependent. FALSE \*\*\*.
- Skipjack is key-agile, as the key schedule is very fast to recompute. TRUE \*\*\*\*
- The operations XOR and addition mod  $2^{32}$  do not commute, so if they are mixed within the definition of a round function, the resulting operation is harder to cryptanalyze. TRUE \*\*\*\*
- Triple-DES with two keys is much more secure than Double-DES. TRUE \*\*\*\*
- Blowfish round function is much simpler to describe than that of DES, involving only the S-boxes, XOR and addition mod  $2^{32}$ . TRUE \*\*\*\*
- For some values of the key, RC4 can be initialized to an internal state that is not a permutation of the values 0 through 255, i.e., some values may appear multiple times. FALSE \*\*\*
- For some values of the key, the S-Boxes of Blowfish may have repeated entries, but that is not likely. TRUE \*\*\*\*
- Skipjack round functions performs only byte operations, being adequate for small word-size processors. TRUE \*\*\*\*
- If the RC4 key is all zeros, the resulting permutation will be the identity permutation. FALSE \*\*\* (See the RC4 Key Schedule algorithm, below.)

```
FOR  $i = 0$  TO 255 DO
     $S[i] = i$ .
 $j = 0$ ;
FOR  $i = 0$  TO 255 DO
     $j = (j + S[i] + K[i \bmod \ell]) \bmod 256$ 
    SWAP( $S[i], S[j]$ )
```

*RC4 Key scheduling algorithm with a key of length  $\ell$ .*

---

7. (21 pts) Choose the right answer.

- The following cipher has the shortest *code*: { Skipjack, RC4 }.
- The following cipher has variable key lengths: { Skipjack, Blowfish }.
- The following cipher is a stream cipher: { RC4, Blowfish }.
- Blowfish has { 16, 32 } rounds and uses { 4, 6 } different S-Boxes.
- The Blowfish round function includes the operation: { expansion-permutation, addition mod  $2^{32}$  }.
- The Skipjack algorithm has { 32, 16 } rounds.

8. (15 pts) Explain the difference between a master key and a session key, and list two reasons why it is important to have a hierarchy of keys, with both master and session keys.

A master key has a long lifetime, while session keys are used to encrypt data in a single (or a few) communication sessions. Some of the reasons to have a key hierarchy are: 1) To limit the amount of data that is encrypted under the same key. 2) Master keys cannot be protected by cryptographic means. The less frequently they are used, the easier it is to maintain them in a secure environment. 3) Some algorithms, such as stream ciphers, require a different key each time. Using the master keys to derive session keys in a pseudo-random fashion allow long-time keys to be used with a stream cipher.