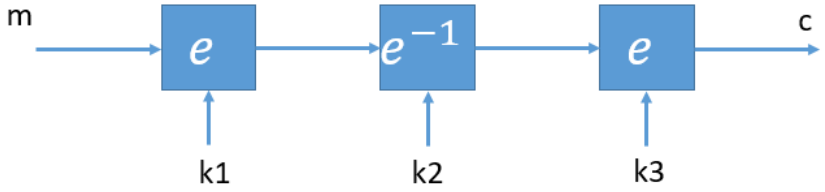
ISEC 2000 Fundamental Concepts of Cryptography
Laboratory 5
@ Computing, Curtin University

Notes:

- Make sure you complete prac questions. Assignments are highly related to them. In fact, programming questions are building blocks for the assignments.
- Group discussion is encouraged but make sure you complete questions individually.
- Ask questions not just answers. There is no answer of prac questions documented or provided for computing units.
- You can use your preferred programming language, C/C++, Java, or Python. Do NOT rely on libraries excessively.

1. When 3DES is built into a hardware device (say a chipset), it is usually implemented in a *encryption-decryption-encryption* fashion: $c = e_{k3}(e_{k2}^{-1}(e_{k1}(m)))$. Can you please think of one advantage of doing this, compared to the way of *encryption-encryption-encryption*?



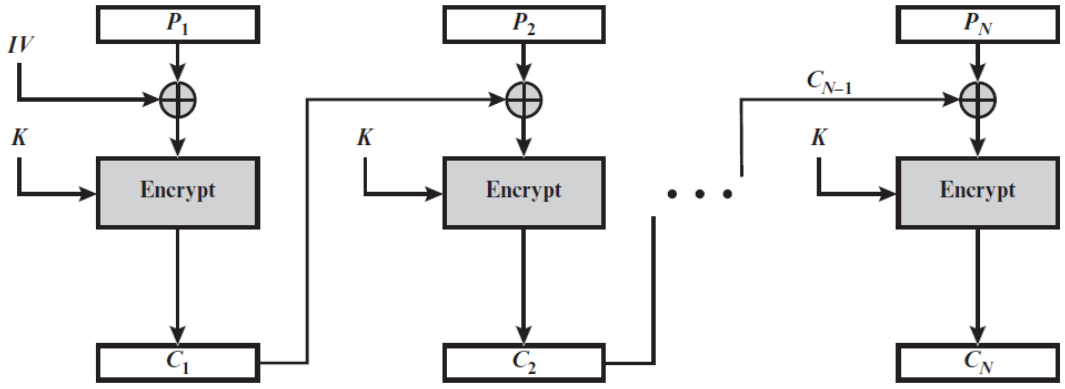
2. With the ECB mode, if there is an error in a block of the transmitted ciphertext, only the corresponding plaintext block is affected. However, in the CBC mode, this error propagates. For example, an error in the transmitted C1 (Figure 7.4) obviously corrupts P1 and P2.

   - Are any blocks beyond P2 affected?
   - Suppose that there is a bit error in the source version of P1. Through how many ciphertext blocks is this error propagated? What is the effect at the receiver?

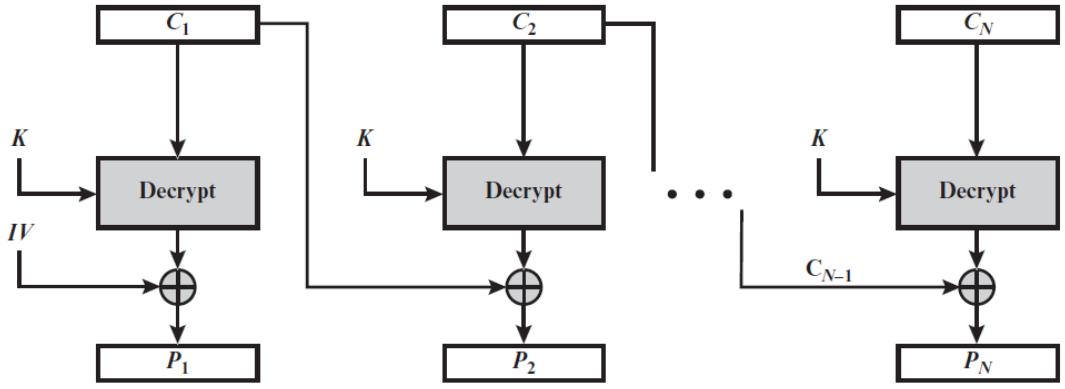
3. One of the challenges of RSA lies in its key schedule, where we need to find two large prime numbers p and q. In practice, we can use probabilistic primality test algorithms, such as the following Lehmann's algorithm. Implement the Lehmann algorithm and use it to find a prime number larger than 10000.

Lehmann Algorithm: to test whether a number p is a prime number.

- Step 1): choose a random number a that is less than p.
- Step 2): calculate $r = a^{\frac{p-1}{2}} \ mod \ p$.
- Step 3): check if r is not 1 or $p-1$, then p is definitely NOT a prime. if $r = 1$ or $r = p-1$, then the probability of p is not a prime is at most $\frac{1}{2}$
- Step 4): Repeat steps 1),2),3) t times, if r equals to 1 or $p-1$ every time but not always equal to 1, then the probability of p being a prime is $1 - \frac{1}{2^t}$.



(a) Encryption



(b) Decryption

Figure 7.4 Cipher Block Chaining (CBC) Mode