A22648

Calculators may be used in this examination provided they are not capable of being used to store alphabetical information other than hexadecimal numbers

THE UNIVERSITY OF BIRMINGHAM

THIS PAGE TO BE REPLACED BY OFFICE

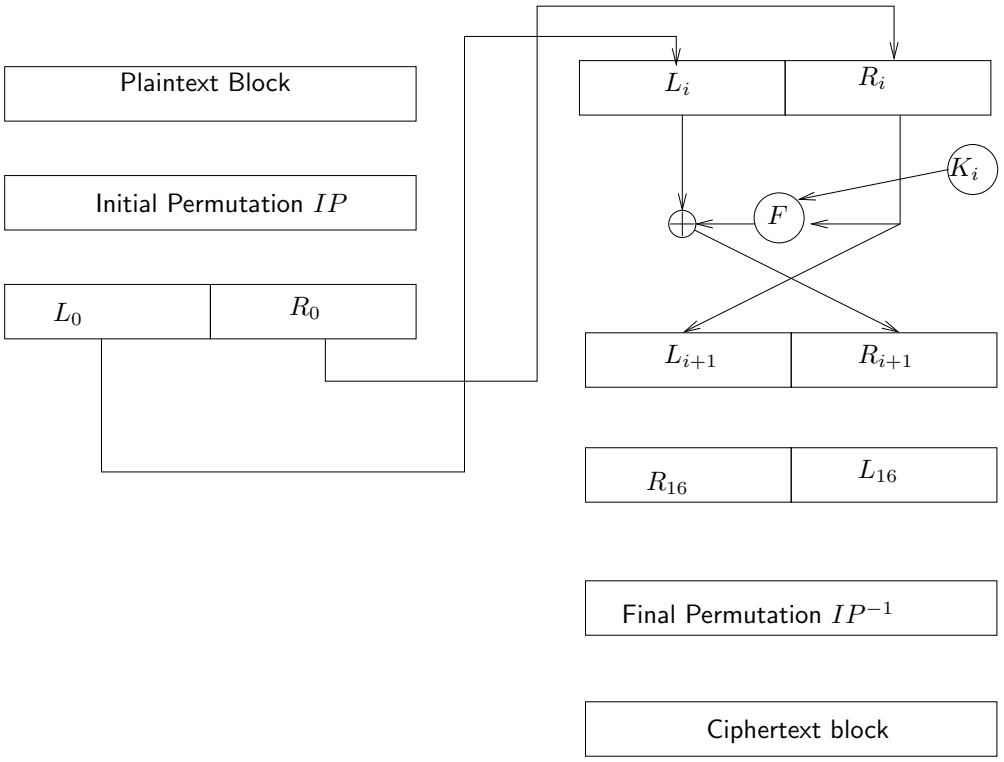
06 00000

Cryptography

May 2018 1.5 hours

[Answer THREE questions (out of a total number of 4 questions). Each question will be marked out of 24. Up to 20 marks will be awarded for content, with up to 4 additional marks for the quality, coherence, and clarity of your answer. The examination will be marked out of 72, which will be rescaled to a mark out of 100.]

1. The diagram below indicates the operation of the Feistel network for the encryption scheme DES.



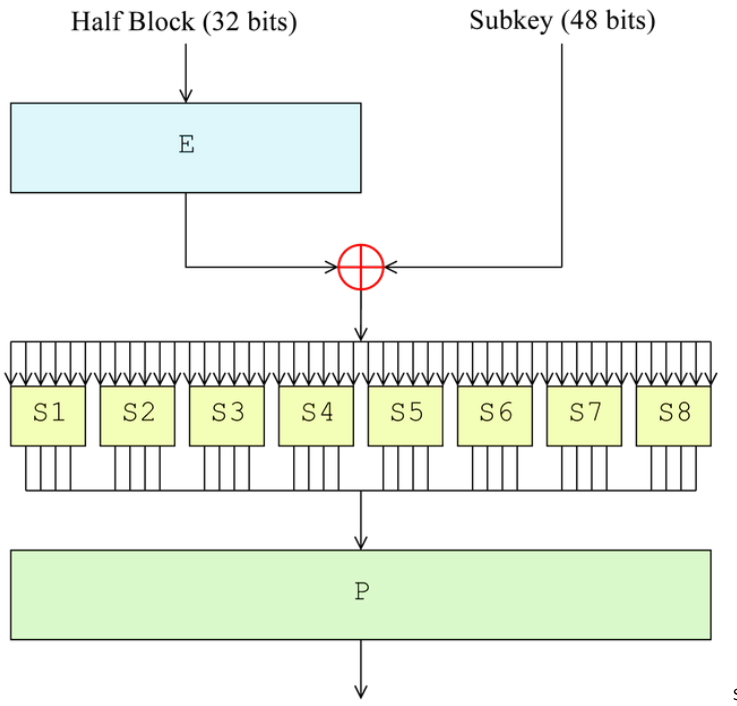
(a) In the context of DES, what is meant by a *subkey* (noted K_i in the diagram)? **[5 points]**

(b) Write down L_{i+1} and R_{i+1} in terms of L_i, R_i, and K_i. **[5 points]**

(c) Using the notation of the diagram, explain how decryption works (that is, how one computes a plaintext block from a ciphertext block and the subkeys $K_0, \ldots, K_{15}$). **[5 points]**

Question 1 continues on the next page.

The DES Feistel function (noted F in the figure of the previous page) is shown in more detail in the figure below.



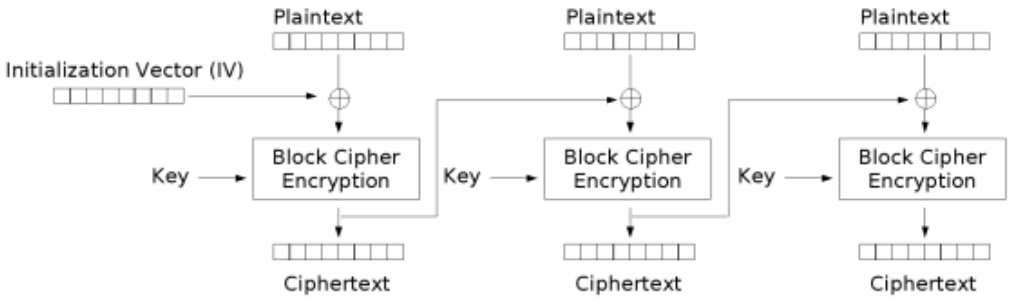
Source: Wikipedia

It takes as input a half-block (32 bits) and a subkey (48 bits), and produces 32 bits of output.

(d) Suppose one has the output (32 bits), and the subkey (48 bits). Can one reconstruct uniquely the 32 bits of input? Explain your answer. **[5 points]**

Additional points to be awarded for quality of the answer. **[4 points]**

2. The figure below is to remind you of the CBC block mode for encryption.



Cipher Block Chaining (CBC) mode encryption

Source: Wikipedia

(a) Using the figure, explain in words how the ciphertext is computed from the plaintext and the key. **[5 points]**

(b) Explain how decryption works; that is, how the plaintext is derived from the ciphertext. Take care to include the role of IV in your explanation. **[5 points]**

(c) Suppose Bob has a file, $f1$, on his hard drive. He makes an exact copy of $f1$, which he calls $f2$. Then he encrypts $f1$, resulting in the file $c1$; and he encrypts $f2$, resulting in the file $c2$. He uses the same encryption key for the two encryptions. His encryption program uses AES in CBC mode. Are the files $c1$ and $c2$ the same? Explain your answer. **[5 points]**

(d) Bob now plans to store $c1$ on an untrusted server. He is concerned that when he later downloads $c1$ from the server and decrypts it, someone may have altered $c1$ and it might decrypt to a different plaintext file, without his being able to detect that. Is that possible? If yes, how? If not, why not? Advise Bob on what he should do to alleviate his concern. **[5 points]**

Additional points to be awarded for quality of the answer. **[4 points]**

3. Let us consider a trapdoor function family $(f_{PK}(\cdot), f_{SK}^{-1}(\cdot))$, where $f_{PK} : X \to Y$ and $f_{SK}^{-1} : Y \to X$ are such that $f_{SK}^{-1}(f_{PK}(x)) = x$ with overwhelming probability for any x in the set X. You can assume f_{PK} is an injective function, namely $f(x_1) = f(x_2)$ implies $x_1 = x_2$.

   (a) Give a precise definition in no more than three sentences of what it means for a trapdoor function family $(f_{PK}(\cdot), f_{SK}^{-1}(\cdot))$ to be *hard to invert*. **[5 points]**

   (b) Define the notion of existential unforgeability for digital signature schemes. **[5 points]**

   (c) Assume the existence of a hash function $H : \{0,1\}^* \to Y$. Describe how to build a secure digital signature scheme from the hash and trapdoor functions. **[5 points]**

   (d) Provide a specific instance of a one-way trapdoor function. Identify the hardness assumption under which your trapdoor function is hard to invert. **[5 points]**

   Additional points to be awarded for quality of the answer. **[4 points]**

4. Let us consider the family of Discrete Logarithm based computational problems with parameters (G, p, q) for large primes p, q, where G has q elements and is a subgroup of $\mathbf{Z}_p^\star$.

   (a) Answer the following questions:

      (i) Is there any relationship between p and q, other than both being prime numbers? If so, describe that relationship.

      (ii) Describe in no more than three sentences the Discrete Logarithm problem.

   [5 points]

   (b) Describe in no more than three sentences the Computational Diffie-Hellman (CDH) problem. Solve the CDH problem on input $(3, 9, 4)$ for group parameters $(G, p, q) := (\langle 3 \rangle, 11, 5)$, where $\langle 3 \rangle$ stands for the subgroup of $\mathbf{Z}_{11}^\star$ generated by 3. Justify your answer. **[5 points]**

   (c) Describe in no more than three sentences the Decisional Diffie-Hellman (DDH) problem. Solve the DDH problem on inputs $(9, 4, 5, 1)$ and $(9, 4, 5, 3)$ for group parameters $(G, p, q) := (\langle 9 \rangle, 11, 5)$, where $\langle 9 \rangle$ stands for the subgroup of $\mathbf{Z}_{11}^\star$ generated by 9. **[5 points]**

   (d) Consider a group (G, p, q) where the CDH is conjectured to be infeasible to solve. You are suggested to work with a cryptosystem with a key generation algorithm as follows:

   - KeyGen(G, p, q) : choose g, h randomly in G and set the public key $PK := (g, h, p, q)$ and the secret key $SK := x$, where x is such that $g = h^x \bmod p$.

   Identify what is wrong with this key generation algorithm. Justify your answer.

   [5 points]

   Additional points to be awarded for quality of the answer. **[4 points]**