Problems

15.1 PGP makes use of the cipher feedback (CFB) mode of CAST-128, whereas most symmetric encryption applications (other than key encryption) use the cipher block chaining (CBC) mode. We have

CBC: \[ C_i = E(K, [C_{i-1} \oplus P_i]) \quad P_i = C_{i-1} \oplus D(K, C_i) \]

CFB: \[ C_i = P_i \oplus E(K, C_{i-1}) \quad P_i = C_i \oplus E(K, C_{i-1}) \]

These two appear to provide equal security. Suggest a reason why PGP uses the CFB mode.

15.2 In the PGP scheme, what is the expected number of session keys generated before a previously created key is produced?

15.3 In PGP, what is the probability that a user with \( N \) public keys will have at least one duplicate key ID?

15.4 The first 16 bits of the message digest in a PGP signature are translated in the clear.
   a. To what extent does this compromise the security of the hash algorithm?
   b. To what extent does it in fact perform its intended function, namely, to help determine if the correct RSA key was used to decrypt the digest?

15.5 In Figure 15.4, each entry in the public-key ring contains an owner trust field that indicates the degree of trust associated with this public-key owner. Why is that not enough? That is, if this owner is trusted and this is supposed to be the owner’s public key, why is not that trust enough to permit PGP to use this public key?

15.6 Consider radix-64 conversion as a form of encryption. In this case, there is no key. But suppose that an opponent knew only that some form of substitution algorithm was being used to encrypt English text and did not guess it was Base64. How effective would this algorithm be against cryptanalysis?

15.7 Phil Zimmermann chose IDEA, three-key triple DES, and CAST-128 as symmetric encryption algorithms for PGP. Give reasons why each of the following symmetric encryption algorithms described in this book is suitable or unsuitable for PGP: DES, two-key triple DES, and AES.