SOLUTION NOTES

Introduction to Security 2003 Paper 3 Question 9 (MGK)

(a) Discretionary access control: Objects such as files and programs are owned by users, who can determine freely (at their discretion) how they want to share these objects with other users, by specifying what access rights others have to their objects.

Mandatory access control: Access to objects is controlled by a system-wide policy, for example a restriction on certain information flows or based on security labels associated with users and objects. Even the owners of objects are restricted by this policy.

(b) (i) CBC is a recommended standard method of encrypting messages that might be longer than the block size of a block-cipher function E. It ensures that the input values provided to E are uniformly distributed and randomised in a way that varies both with the block position and with each application of CBC. CBC first outputs a single block C_0 of random bits. It then pads and splits the message into plaintext blocks $P_1, \ldots, P_n$ and outputs the ciphertext blocks $C_i = E_K(P_i \oplus C_{i-1})$, where $\oplus$ is the bitwise exclusive-or of two blocks.

(ii) Use

$$P_i = D(C_i) \oplus C_{i-1}$$

where D is the decryption function for block cipher E.

(c) (i) Generate a key pair (K, K^{-1}) for an asymmetric crypto system (e.g., ElGamal or RSA). Store the public key K in the camera and keep the private key K^{-1} at home. While recording, generate in regular intervals (e.g., every few minutes) randomly a new session key S_i. Use it with a fast symmetric cipher to encrypt the compressed digital video signal. Save $\{S_i\}_K$ with this data and then overwrite S_i in the camera's memory carefully before generating the next session key S_{i+1}. Only the private key K^{-1} at home can recover the session keys needed to decrypt the video stream.

(ii) Generate a random value S_0 and save it both at home and in the camera. Use S_0 as the session key to encrypt the first recording interval and save the interval number 0 with it. At the beginning of a new interval i, calculate $S_i = h(S_{i-1})$, where h is a one-way function. Then overwrite in the camera's memory any trace of S_{i-1} and use S_i as the new session key. Earlier session keys cannot be derived from the current one. Only the first session key S_0 at home can reconstruct the entire hash chain of session keys S_i.

Coverage: This question refers mainly to the course chapters on “discretionary and mandatory access control”, “modes of operation”, “secure hash functions”, “public key cryptography” and “hybrid cryptography”.