6 Cryptography (mgk25)

(*a*) *CrashHash* is a cryptographic hash function invented by your colleague this morning. It zero-pads input X, splits it into n 256-bit blocks $x_1 \| x_2 \| \ldots \| x_n = X \| 0^{(-|X|) \bmod 256}$ and then appends a length-indicator block $x_{n+1} = \langle |X| \rangle$, as in the Merkle–Damgård construction. It then iterates a 512-bit to 256-bit compression function of the form $C(K, M) = E_K(M)$, where $E_K(M)$ is a blockcipher E applied with 256-bit key K to 256-bit message block M, as

$$z_1 = C(\langle 0 \rangle, x_1)$$
$$z_i = C(z_{i-1}, x_i) \qquad (1 < i \leq n+1)$$

The value $H(X) = z_{n+1}$ is the hash value returned. Show that *CrashHash* is not collision resistant, even if E is replaced with an *ideal cipher*. [6 marks]

(*b*) (*i*) How can one modify an implementation of the DES encryption function to obtain the decryption function? [4 marks]

(*ii*) Name two other features of DES that made it well suited for hardware implementation. [2 marks]

(*c*) Your colleague has generated a set of $m = 200\,000$ RSA key pairs that include a modulus $n_i = p_i q_i$ where p_i and q_i are 1536-bit prime numbers (for $1 \leq i \leq m$). The corresponding p_i and q_i values were discarded immediately after key generation and are no longer available.

Due to a bug in your colleague's key-generation software, two types of fault have appeared in a random subset of the issued key pairs:

(*i*) For some key pairs i we have $p_i = q_i$.

(*ii*) For some key pairs i there exists another key pair j in that set with $p_i = p_j$ and $i \neq j$.

Suggest practical tests that can identify all public keys affected by either of these problems and state how often the algorithms involved have to be executed for this task. [4 marks]

(*d*) Calculate $7^{2000} \bmod 100$ by hand. [4 marks]