3 Cryptography (mgk25)

(*a*) *YottaVPN*, your employer's main network-encryption product, generates a master key $K \in_R \{0,1\}^{128}$ and an initial seed $R_0 \in_R \{0,1\}^{80}$ randomly once, when the product is installed. It then uses

$$\text{Algorithm (A):} \qquad R_i = \mathsf{Enc}_K(R_{i-1}) \qquad \text{for } i > 0$$

to generate a stream $R_1, R_2, \ldots$ of session keys for encrypting individual network connections. That algorithm then runs continuously throughout the lifetime of the product. Your colleague suggests to replace (A) with

$$\text{Algorithm (B):} \qquad R_i = \mathsf{Enc}_K(R_{i-1}) \oplus R_{i-1} \quad \text{for } i > 0$$

because they feel that would be more secure. [Enc is a government-approved blockcipher with 80-bit blocksize and $\oplus$ is bit-wise exclusive-or.]

(*i*) For each of algorithm (A) and (B), averaged over all (K, R_0), what is the expected number of different session keys $|\{R_1, R_2, \ldots\}|$ that they will be able to generate from one (K, R_0)? State your assumptions. [5 marks]

(*ii*) What is the smallest number of different values $|\{R_1, R_2, \ldots\}|$ that could be generated by (A) and (B) from any fixed pair (K, R_0)? [2 marks]

(*iii*) Suggest another deterministic key-derivation algorithm (C), using the same blockcipher, 80-bit state and fixed parameters (K, R_0), that maximises $|\{R_1, R_2, \ldots\}|$. [2 marks]

(*iv*) Years later, a worried user discovers that, due to an operator error, the state (K, R_{65535}) of their *YottaVPN* installation was accidentally committed to a publicly accessible Git repository. Compare which other values R_i were compromised by this leak, if either algorithm (A), (B), or (C) had been used. [6 marks]

(*v*) Name a security benefit that could be claimed for algorithm (B) compared to (A). [1 mark]

(*b*) Your colleagues designed a scheme that encrypts messages $M_i \in \{0,1\}^\ell$ with one-time pads $R_i \in_R \{0,1\}^\ell$ into ciphertexts $C_i = M_i \oplus R_i$. But to help estimate the frequency of transmission errors when transferring the R_i, they decided to occasionally replace the last random bit of any R_i with a "parity" bit, with a probability of 0.01. As a result, the probability of any R_i containing an even number of one bits is 0.505. Does this encryption scheme offer *indistinguishability in the presence of an eavesdropper*? Explain your answer. [4 marks]