Problem Set 7 – Dew 30 May 2024 at 11am

Problem 20. Do the following without a calculator or computer, showing your work. None should be overly tedious. **(a)** Compute $7^{890002} \bmod 1111$. Note that 1111 is the product of primes $p = 11$ and $q = 101$. **(b)** Compute $7^{890002} \bmod 101$. **(c)** Compute $2^{64} \bmod 101$.

Problem 21. Consider the following "left-or-right" security notion for a public-key encryption scheme $\Pi = (\mathcal{K}, \mathcal{E}, \mathcal{D})$:

$$\mathbf{Adv}^{\mathrm{lr}}_{\Pi}(A, k) \;=\; \Pr[(pk, sk) \twoheadleftarrow \mathcal{K}(k) \colon A^{\mathcal{E}(pk, \mathrm{L}(\cdot,\cdot))}(pk) \Rightarrow 1] - \Pr[(pk, sk) \twoheadleftarrow \mathcal{K}(k) \colon A^{\mathcal{E}(pk, \mathrm{R}(\cdot,\cdot))}(pk) \Rightarrow 1]$$

where oracle $\mathrm{L}(X, Y)$ returns X when $|X| = |Y|$; oracle $\mathrm{R}(X, Y)$ returns Y when $|X| = |Y|$; and both oracles return $\perp$ when $|X| \neq |Y|$. In contrast, our old security notion was

$$\mathbf{Adv}^{\mathrm{ind}}_{\Pi}(A, k) \;=\; \Pr[(pk, sk) \twoheadleftarrow \mathcal{K}(k) \colon A^{\mathcal{E}(pk, \cdot)}(pk) \Rightarrow 1] - \Pr[(pk, sk) \twoheadleftarrow \mathcal{K}(k) \colon A^{\mathcal{E}(pk, 0^{|\cdot|})}(pk) \Rightarrow 1]$$

Show that lr-security is equivalent to ind-security.

Problem 22. Let $\Pi = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ be a public-key encryption scheme. Can it be ind-secure with each of the following "defects"? Briefly justify each answer you give.

Part A. Encryption of a plaintext M leaks the last bit of M — it is easily computable from the ciphertext C.

Part B. Encryption of a plaintext M leaks the length of M — it is easily computable from the ciphertext C.

Part C. Encryption of a plaintext M leaks the identity of the key pk with which it is encrypted—it is easy to distinguish if a given ciphertext was meant for Alice (it's encrypted under her key) or for Bob (it's encrypted under his).

Part D. Encryption of equal-length plaintexts M and M' can take radically different amounts of time.

Part E. Encryption of the secret key sk under its public key pk leaks sk — it is easily computable from the ciphertext C.