d. Same as conditions a–c with the roles of the two countries reversed.
e. The verification devices in both countries must be identical, and must be constructed jointly by scientists from both countries.

4. The purpose of this problem is to construct a long–distance coin flip using any two-to-one trapdoor function. For example, suppose that two chess players at distant parts of the world are playing chess by mail or telephone and want a fair way to determine who plays white. Or suppose that when making preparations for an international ice–hockey match, representatives of the two teams decide to flip a coin to see which country hosts the match, without having to arrange a meeting (or trust a third party) to "flip the coin."
By a system of two-to-one trapdoor functions, we mean an algorithm which, given a key K_E of a suitable type, constructs a function $f: \mathcal{P} \longrightarrow \mathcal{C}$ such that every element c in the image of f has exactly two preimages $p_1, p_2 \in \mathcal{P}$ such that $f(p_j) = c$; and an algorithm which, given a key K_D which "reverses K_E," can find both preimages of any c in the image of f. Here we assume that it is computationally infeasible to find K_D knowing only K_E. Given an element $p_1 \in \mathcal{P}$, notice that one can find the other element p_2 having the same image if one knows both K_E and K_D (namely, find both inverses of $f(p_1)$); but we assume that, knowing only K_E, one cannot feasibly compute the companion element p_2 for *any* p_1 at all.
Suppose that Player A (Aniuta) and Player B (Björn) want to use this set-up to flip a coin. Aniuta generates a pair of keys K_E and K_D and sends K_E (but *not* K_D) to Björn. Explain a procedure that has a 50%–50% chance of each player "winning" (give a suitable definition of "winning"), and that has adequate safeguards against cheating.

References for § IV.1

1. M. Blum, "Coin-flipping by telephone — a protocol for solving impossible problems," *IEEE Proc., Spring Compcon.*, 133–137.
2. W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory IT-22* (1976), 644–654.
3. D. Chaum, "Achieving electronic privacy," *Scientific American*, **267** (1992), 96–101.
4. S. Goldwasser, "The search for provably secure cryptosystems," *Cryptology and Computational Number Theory, Proc. Symp. Appl. Math.* **42** (1990), 89–113.
5. M. E. Hellman, "The mathematics of public-key cryptography," *Scientific American*, **241** (1979), 146–157.
6. E. Kranakis, *Primality and Cryptography*, John Wiley & Sons, 1986.
7. R. Rivest, "Cryptography," *Handbook of Theoretical Computer Science*, Vol. A, Elsevier, 1990, 717–755.