4. Björn chooses at random an element $p \in \mathcal{P}$, computes $c = f(p)$ and sends Aniuta c. Aniuta then computes the two preimages p_1 and p_2 and sends only one of them, say p_1, to Björn. If $p_1 \neq p$, then Björn can name both preimages p_1 and $p_2 = p$, in which case we say that Björn wins; otherwise, Aniuta wins. If Aniuta wins, she has to produce the second preimage, which Björn can verify does in fact satisfy $f(p_2) = c$ (otherwise, Aniuta could cheat by choosing an improper key, for which each c has only one preimage). (Aniuta would have no interest in choosing a key for which each c has more than two preimages, since that would just lessen her chances of sending Björn the preimage that he already knows.)

§ IV.2.

1. (a) BH A 2AUCAJEAR0; (b) $2047 = 23 \cdot 89$ (see Example 1 in § I.4), $d_A = 411$; (c) since $\varphi(23)$ and $\varphi(89)$ have small least common multiple 88, any inverse of 179 modulo 88 will work as d_A (e.g., 59).
2. n_A is the product of the Mersenne prime 8191 and the Fermat prime 65537 — a flamboyantly bad choice; $d_A = 201934721$; "DUMPTHESTOCK."
3. (a) STOP PAYMENT; (b) (i) 6043; (ii) $n = 113 \cdot 191$.
4. On the third try $t = 152843, 152844, 152845$ you find that $t^2 - n = 804^2$ and so $p = 152845 + 804 = 153649$, $q = 152845 - 804 = 152041$.
5. To show that one cannot feasibly compute the companion element in $\mathcal{P}$ that has the same image as a given element, we suppose that a person who knows only K_E (i.e., knows n but not its factorization) obtained a second pair $\pm x_2$ with the same square modulo n as $\pm x_1$. Then show that $g.c.d.(x_1 + x_2, n)$ is either p or q. In other words, finding a *single* pair of companion elements of $(\mathbf{Z}/n\mathbf{Z})^*/\pm 1$ is tantamount to factoring n.
6. It suffices to prove that $a^{de} \equiv a \bmod p$ for any integer a and each prime divisor p of n. This is obvious if $p|a$; otherwise use Fermat's Little Theorem (Proposition I.3.2).
7. If $m/2 \equiv (p-1)/2 \bmod p-1$, then $a^{m/2} \equiv (\frac{a}{p})$, which is +1 half the time and −1 half the time. In case (ii), use the Chinese Remainder Theorem to show that the probability that an element in $(\mathbf{Z}/n\mathbf{Z})^*$ is a residue modulo p and the probability that it is a residue modulo q are independent of one another, i.e., the situation in case (ii) is like two independent tosses of a coin.

§ IV.3.

1. (a) 24, 30, 11, 13; (b) 1, $\alpha^2 + \alpha$, α, $\alpha + 1$.
2. (i) To justify moving the a to the left, notice that if $x < \varphi(3^\alpha)$ is the solution of $2^x a \equiv 1 \bmod 3^\alpha$, then $\varphi(3^\alpha) - x$ is the solution of the original congruence. If $a \equiv 2 \bmod 3$, then solve the problem $2^x(2a) \equiv 1 \bmod 3^\alpha$, in which we do have $2a \equiv 1 \bmod 3$, and then $x + 1$ is the solution of the original congruence. If $a \equiv 1 \bmod 3$, then the solution x must be even,