RSA Algorithm
(Rivest, Shamir, Adelman, 1977)

• Choose two large prime numbers (e.g., > $10^{100}$) $p_A$ and $q_A$
• Compute $n_A = p_A \times q_A$
• Compute $z_A = (p_A - 1) \times (q_A - 1)$
• Choose a number $e_A$ relatively prime to $z_A$, s.t. $1 < e_A < z_A$
• Choose $d_A$ such that $d_A \times e_A = 1 \mod z_A$
or $d_A = e_A^{-1} \mod z_A$

RSA (cont)

• Public Key:
• Deciphering Key:
• Enciphering transformation:
  $E_k = f(P) = C = $
• Deciphering transformation:
  $D_k = f^{-1}(C) = = P$
• Write theorem that justifies that the deciphering transformation works: