Rotors need to have randomized alphabet order, otherwise keys “MAS” and “SSS” for example result in the ciphertext because ?

(Lyons, 2014)

Entry points (Oberzalek, 2000)

* The three letters are not really random (e.g. AAA, initials of girlfriend)
* A letter never encrypts itself (e.g. a will never become A)
* Cribs: first few letters were known, e.g. “An General …”/”An die Gruppe” 🡪 “Anx…”
* Turing bomb: test all possible 26\*26\*26 cases
  1. Assume current setting is the correct one
  2. Try to disprove it (e.g. plaintext letter encodes to same letter)