1. Symmetric key ciphers

- **Symmetric key cipher**: one in which encryption and decryption keys are equal.
- **Key size**: $\log_2$(number of possible keys).
- **Caesar cipher**: shift all characters by a constant amount. Key size is $\log_2(26)$
- **Substitution cipher**: key is permutation of $\{a, ..., z\}$. Key size is $\log_2(26!)$.
- **Stirling's formula**:

$$n! \approx \sqrt{2\pi n}\left(\frac{n}{e}\right)^n$$

- If any statistical properties of plaintext are reflected in cipher text, then we can use this as basis for an attack. We compare the most common letters in the English language with the most common letters in the message. We can also compare letter pairs.