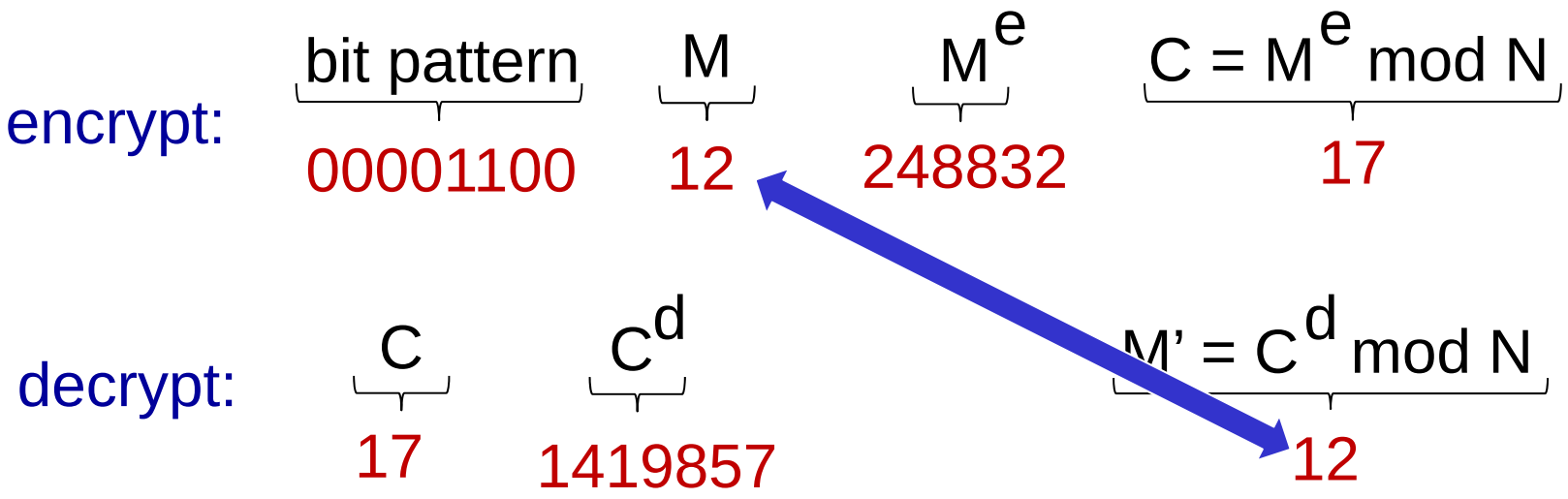
RSA Toy Example

- Bob chooses $p = 5, q = 7$.
- Then $N = 35, \phi(n) = 24$.
- Suppose $e = 5$ is chosen (so $e, \phi(n)$ are co-prime)
- Compute $d = 5$ (by xgcd so that $ed \equiv 1 \pmod{\phi(n)}$)
- Encrypt 8-bit message



In practice, the numbers are very large.
Fast exponentiation is used instead!