# ❖ Algorithm Reference sheet

**Algorithm 1** Period Finding

1: Start with $|0\ldots0\rangle\,|0\ldots0\rangle$ (We refer to these as first and second register, each have $n$ qubits)
2: Apply $H^{\otimes n}$ on the first register to get $\frac{1}{\sqrt{N}}\sum_{y=0}^{N-1}|y\rangle\,|0\rangle$
3: Apply $U_f$
4: Measure the 2nd register.
5: Ignore the 2nd register and apply $QFT_N$ to the 1st register.
6: Measure the 1st register to get value $a$.
7: Postprocessing: Use $a$ and $N$ to find $k$ and $r$.

**Algorithm 2** Factoring

1: Pick $x$ at random from $\{2,\ldots,M-1\}$
2: **if** $\gcd(x,M)\neq 1$ **then**
3: $\gcd(x,M)$ is a non-trivial factor of $M$ so we are done!
4: **else**
5: Use quantum Period Finding algorithm (alg 1) to find smallest $s$ such that $x^s = 1 \mod M$.
6: Call this variable $r$.
7: **if** $r$ is odd **then**
8: Start over..
9: **else if** $x^{r/2} = \pm 1 \mod M$ **then**
10: Start over..
11: **else**
12: $x^{r/2} \mod M$ is a non-trivial square root of 1 mod $M$
13: **end if**
14: **end if**
15: Postprocessing: Compute $\gcd(x^{r/2}-1,M$ and $\gcd(x^{r/2}+1,M$ to find the factors of $M$.

## ❖ Scratch paper

## ❖ Scratch paper

## ❖ Scratch paper