$\boxed{\text{RSA}}$ The set up: Key generation.

1. Pick 2 big primes p, q (Ex: $p=59$, $q=73$)
2. Let $n=pq$ ($n=4307$)
3. Find $\phi(n)=(p-1)(q-1)$ ($\phi(n)=58 \cdot 72=4176$)
4. Pick e coprime with $\phi(n)$ ($e=19$)
5. Calculate d such that $ed \equiv 1 \pmod{\phi(n)}$
   (This exists since $\gcd(e, \phi(n))=1$.)
   ($19d \equiv 1 \pmod{4176}$, $d=1099$)

Public key: (e, n)

Private key: (d, n)

How it works

Encryption: Message M satisfies $0 \leq M < n$

Calculate $C \equiv M^e \pmod{n}$ (remainder of M^e div. by n)

C = ciphertext, send to receiver.

Decryption: Calculate $D \equiv C^d \pmod{n}$ D = decrypted msg.

To be successful, need $D=M$

Example: $(e, n)=(19, 4307)$ $(d, n)=(1099, 4307)$

Message: TED $\rightarrow$ $\underset{M_1}{2005} / \underset{M_2}{04}$

Encrypt: $C \equiv 2005^{19} \pmod{4307}$

$C=1356$

Decrypt: $D=C^d=1356^{1099} \pmod{4307}$

$D=2005$

Theorem in RSA, $D \equiv M \pmod{n}$

Proof: $D \equiv C^d \pmod{n} \equiv M^{ed} \pmod{n}$

(Goal $M \equiv M^{ed} \pmod{n}$)

Now $n = pq$ and $\gcd(p,q) = 1$, so we split the modulus into mod p and mod q.

(mod p): Goal $M \equiv M^{ed} \pmod{p}$

Recall: $ed \equiv 1 \pmod{\phi(n)} \equiv 1 \pmod{(p-1)(q-1)}$.

So $ed = 1 + k(p-1)(q-1)$ for some $k \in \mathbb{Z}$.

Suppose $p \nmid M$. By FLT, $M^{p-1} \equiv 1 \pmod{p}$

$$
\begin{aligned}
\text{So } M^{ed} &\equiv M^{1+k(p-1)(q-1)} \pmod{p} \\
&\equiv M\left(M^{p-1}\right)^{k(q-1)} \pmod{p} \\
&\equiv M \pmod{p}
\end{aligned}
$$

If $p \mid M$, $M \equiv 0 \pmod{p}$, $M^{ed} \equiv 0 \pmod{p}$

So $M \equiv M^{ed} \pmod{p}$

So $M \equiv M^{ed} \pmod{p}$ in all cases.

By switching the roles of p and q in the proof above, we get $M \equiv M^{ed} \pmod{q}$.

So $\begin{cases} M \equiv M^{ed} \pmod{p} \\ M \equiv M^{ed} \pmod{q} \end{cases}$ since $\gcd(p,q) = 1$, by CRT,

$$
\begin{aligned}
M &\equiv M^{ed} \pmod{pq} \\
&\equiv M^{ed} \pmod{n} \quad \square
\end{aligned}
$$