issue	private key	public key
1. base theorem	Fermat: $a^{p-1} \equiv 1 \pmod{p}$;	Euler: $a^{\varphi(m)} \equiv 1 \pmod{m}$
	$a < p; p(prime)$	$a \in \text{residues}(m) \doteq r\,(m)$
		$GCD\,(a, m) = 1$
		$\varphi\,(m) = m \prod_{p\|m} \left(1 - \frac{1}{p}\right)$
		where $p\|m$ are the distinct prime factors of m
2. proof sketch	$1a, 2a, \ldots, (p-1)\,a$	$r_1\,(m)\,a, r_2\,(m)\,a, \ldots, r_{\varphi(m)}\,(m)\,a$
	$\equiv 1, 2, \ldots, (p-1) \pmod{p}$	$\equiv r_1\,(m)\,, r_2\,(m)\,, \ldots, r_{\varphi(m)}\,(m) \pmod{m}$
	in some order then products:	in some order then products:
	$(p-1)!a^{p-1} \equiv (p-1)!(\text{mod}\,p)$	$\prod_{i=1}^{\varphi(m)} ar_i\,(m) \equiv \prod_{i=1}^{\varphi(m)} r_i\,(m) \pmod{m}$
	$a^{p-1} \equiv 1 \pmod{p}$	$a^{\varphi(m)} \prod_{i=1}^{\varphi(m)} r_i\,(m) \equiv \prod_{i=1}^{\varphi(m)} r_i\,(m) \pmod{m}$
		$a^{\varphi(m)} \equiv 1 \pmod{m}$

issue	private key	public key
3.encryption		
a. public disclosure	nothing	sender announces e
	(e and p privately communicated)	receiver announces m
		$m = r * s * t$
		$\varphi(m) = rst\left(1-\frac{1}{r}\right)\left(1-\frac{1}{s}\right)\left(1-\frac{1}{t}\right)$
		$= rst\left(\frac{r-1}{r}\right)\left(\frac{s-1}{s}\right)\left(\frac{t-1}{t}\right)$
		$= (r-1)(s-1)(t-1)$
b. decryptor	$.a^{(p-1)n+1} \equiv a(\mathrm{mod}\, p)$	$a^{\varphi(m)n+1} \equiv a\,(\mathrm{mod}\ m)$
	$(a^e)^d = a^{ed} \equiv a\,(\mathrm{mod}\, p)$	$a^{ed} \equiv a\,(\mathrm{mod}\, m)$
	$ed = (p-1)n+1$ $ed \equiv 1(\mathrm{mod}\, p-1)$	$ed = \varphi(m)n+1$ $ed \equiv 1\,(\mathrm{mod}\, \varphi(m))$
	$e^{-1} \equiv d(\mathrm{mod}\, p-1)$	$e^{-1} \equiv d\,(\mathrm{mod}\, \varphi(m))$
c. encoding	text$\rightarrow a$	text$\rightarrow a$
encrypting	$a^e \equiv cyphertext\,(\mathrm{mod}\, p)$	$a^e \equiv cyphertext\,(\mathrm{mod}\, m)$
decrypting	$(a^e)^d \equiv a\,(\mathrm{mod}\, p)$	$(a^e)^d \equiv a\,(\mathrm{mod}\, m)$
decoding	$a \rightarrow$ text	$a \rightarrow$ text