Encrypt

(14) $p = 137$ $q = 241$

$\phi = (p-1)(q-1) = (136)(240) = 32640$

$e = 53$ $n = pq = (137)(241) = 33017$

$a^e \text{ in } Z_n = 12345^{53} \text{ in } Z_{33017}$

$a^n = a^{n/2} \cdot a^{n/2} = (a^{n/2})^2$

12345^{53}

12345 53 12345

12345^2

(1)	$12345^1 =$	$12345 \bmod 33017$
2	$12345^2 =$	$25570 \bmod 33017$
(4)	$12345^4 =$	$22266 \bmod 33017$
8	$12345^8 =$	$24501 \bmod 33017$
(16)	$12345^{16} =$	$16924 \bmod 33017$
(32)	$12345^{32} =$	$32318 \bmod 33017$

$32 \quad 16 \quad 4 \quad 1$

$(32318 \cdot 16924) \cdot 22266 \cdot 12345$

$23727 \; (22266) \; 0 \; 12345$

$(21111 \cdot 12345)$

$= \boxed{24903}$

$C = 24903$

Decode $e = 53$ ϕ 32640

$53x + 32640y = 1$

	a	b	r	q	
	32640	53	45	615	$32640 = 615 \times 53 + 45$
	53	45	8	1	$53 = 1 \times 45 + 8$
	45	8	5	5	$45 = 5 \times 8 + 5$
	8	5	3	1	$8 = 1 \times 5 + 3$
	5	3	2	1	$5 = 1 \times 3 + 2$
	3	2	1	1	$3 = 1 \times 2 + 1$
gcd	2	1	0	2	
	1	0	—	—	

$1 = s\phi + de$

	ϕ	e					
	a	b	= p	q	s	d	
	32640	53	45	615	-20	12317	$1 = (-20)32640 + d(53)$
	53	45	8	1	17	-20	$1 = (17)(53) + d(45)$
	45	8	5	5	-3	17	$1 = (-3)45 + d(8)$
	8	5	3	1	2	-3	$1 = (2)(8) + d(5)$
	5	3	2	1	-1	2	$1 = (-1)(5) + d(3)$
	3	2	1	1	1	-1	$1 = (1)(3) + d(2)$
gcd	2	1	0	2	0	1	$1 = (0)(2) + (1)(1)$
	1	0	—	—	1	0	$1 = (1)(1) + 0(0)$

$d = 12317$

$n = 33017$

$c = 24983$