RSA

N = 11363
E = 211

11363 = 11 X 1033

P=11, Q=1033

$\emptyset = (p-1)(q-1)$

$\emptyset = 10320$

$D= E^{-1} \bmod \emptyset(n)$

$D= 211^{-1} \bmod 10320$

$D= E^{-1} \bmod \emptyset(n)$
N= P x Q
$CT = PT^{E} \bmod N$
$PT = CT^{D} \bmod N$

$211^{-1} \bmod 10320$

Q	R1	R2	R	T1	T2	T (T1-QT2)
48	10320	211	192	0	1	-48
1	211	192	19	1	-48	49
10	192	19	2	-48	49	-538
9	19	2	1	49	-538	4891
2	2	1	0	-538	4891	

$D = 211^{-1} \bmod 10320$

$D = 4891$

P=11
Q=13
E=17

M= FA = 50

N= P x Q = 143

$CT = PT^{E} \bmod N$

$CT = 50^{17} \bmod 143$

17 => 10001

$50^{1} \bmod 143 = 50$
$50^{2} \bmod 143 = 69$
$69^{2} \bmod 143 = 42$
$42^{2} \bmod 143 = 48$
$48^{2} \bmod 143 = 16$

$16 \times 50 \bmod 143 = 85$

$PT = CT^{D} \bmod N$

$D = E^{-1} \bmod \phi(n)$

$D = 17^{-1} \bmod 120$

$17^{-1} \bmod 120$

Q	R1	R2	R	T1	T2	T = T1-QT2
7	120	17	1	0	1	-7
17	17	1	0	1	-7	

$D = 120-7 = 113$

$PT = 85^{113} \bmod 143$

$113 \Rightarrow 1110001$

$85 \bmod 143 = 85$

$85^{2} \bmod 143 = 75$

$75^{2} \bmod 143 = 48$

$48^2 \bmod 143 = 16$
$16^2 \bmod 143 = 113$
$113^2 \bmod 143 = 42$
$42^2 \bmod 143 = 48$

$48 \times 42 \bmod 143 = 14$
$14 \times 113 \times 85 \bmod 143 = 50$

PT = 50

PT = PT

$13^{-1} \bmod 83$

Q	R1	R2	R	T1	T2	T = T1-QT2
6	83	13	5	0	1	-6
2	13	5	3	1	-6	13
1	5	3	2	-6	13	-19
1	3	2	1	13	-19	32
2	2	1	0	-19	32	

$13^{-1} \bmod 83 = 32$