RSA Algorithm Example

- Choose $p = 3$ and $q = 11$
- Compute $n = p * q = 3 * 11 = 33$
- Compute $\phi(n) = (p - 1) * (q - 1) = 2 * 10 = 20$
- Choose e such that $1 < e < \phi(n)$ and e and ϕ (n) are coprime. Let $e = 7$
- Compute a value for d such that $(d * e) \% \phi(n) = 1$. One solution is $d = 3$ [(3 * 7) % 20 = 1]
- Public key is (e, n) => (7, 33)
- Private key is (d, n) => (3, 33)
- The encryption of $m = 2$ is $c = 2^7 \% 33 = 29$
- The decryption of $c = 29$ is $m = 29^3 \% 33 = 2$

RSA Encryption

$N = p \cdot q \mid p \wedge q$ are prime #'s

$\phi(N) = (p-1)(q-1) = r$ Eulers Totient

$e \cdot d \% r = 1 \rightarrow e^{-1} = d \vee d^{-1} = e$

then

$C = M^e \% N \rightarrow$ Encrypted Message

$A = C^d \% N \rightarrow$ Decrypted ″

$A = C^d \% N = M^{ed} \% N$ = Original Message

$= M^{\phi(N)+1} \% N = M$ Eulers Theorem