

RSA Demonstration		X RSA Demonstration	
RSA using the private and public key -- or using only the public key <input checked="" type="radio"/> Choose two prime numbers p and q. The composite number N = pq is the public RSA modulus, and phi(N) = (p-1)(q-1) is the Euler totient. The public key e is freely chosen but must be coprime to the totient. The private key d is then calculated such that d = e ⁻¹ (mod phi(N)). <input type="radio"/> For data encryption or certificate verification, you will only need the public RSA parameters: the modulus N and the public key e.		RSA using the private and public key -- or using only the public key <input checked="" type="radio"/> Choose two prime numbers p and q. The composite number N = pq is the public RSA modulus, and phi(N) = (p-1)(q-1) is the Euler totient. The public key e is freely chosen but must be coprime to the totient. The private key d is then calculated such that d = e ⁻¹ (mod phi(N)). <input type="radio"/> For data encryption or certificate verification, you will only need the public RSA parameters: the modulus N and the public key e.	
Prime number entry Prime number p <input style="width: 100px;" type="text" value="61"/> Prime number q <input style="width: 100px;" type="text" value="53"/> <button style="margin-top: 5px;">Generate prime numbers...</button>		Prime number entry Prime number p <input style="width: 100px;" type="text" value="61"/> Prime number q <input style="width: 100px;" type="text" value="53"/> <button style="margin-top: 5px;">Generate prime numbers...</button>	
RSA parameters RSA modulus N <input style="width: 100px;" type="text" value="3233"/> (public) phi(N) = (p-1)(q-1) <input style="width: 100px;" type="text" value="3120"/> (secret) Public key e <input style="width: 100px;" type="text" value="65537"/> Private key d <input style="width: 100px;" type="text" value="2753"/> <button style="margin-top: 5px;">Update parameters</button>		RSA parameters RSA modulus N <input style="width: 100px;" type="text" value="3233"/> (public) phi(N) = (p-1)(q-1) <input style="width: 100px;" type="text" value="3120"/> (secret) Public key e <input style="width: 100px;" type="text" value="65537"/> Private key d <input style="width: 100px;" type="text" value="2753"/> <button style="margin-top: 5px;">Update parameters</button>	
RSA encryption using e / decryption using d [alphabet size: 256] Input as <input checked="" type="radio"/> text <input type="radio"/> numbers <button style="margin-top: 5px;">Alphabet and number system options...</button> Input text <input style="width: 100px;" type="text" value="helloworld"/> The Input text will be separated into segments of Size 1 (the symbol '#' is used as separator). <input style="width: 100px;" type="text" value="h#e#l#l#w#o#r#d#"/> Numbers input in base 10 format. <input style="width: 100px;" type="text" value="104#101#108#108#111#119#111#114#108#100"/> Encryption into ciphertext c[i] = m[i]^e (mod N) <input style="width: 100px;" type="text" value="2170#1313#0745#0745#2185#1107#2185#2412#0745#1773"/>		RSA encryption using e / decryption using d [alphabet size: 256] Input as <input type="radio"/> text <input checked="" type="radio"/> numbers <button style="margin-top: 5px;">Alphabet and number system options...</button> Ciphertext coded in numbers of base 10 <input style="width: 100px;" type="text" value="2170#1313#0745#0745#2185#1107#2185#2412#0745#1773"/> Decryption into plaintext m[i] = c[i]^d (mod N) <input style="width: 100px;" type="text" value="0104#0101#0108#0108#0111#0119#0111#0114#0108#0100"/> Output text from the decryption [into segments of size 1; the symbol '#' is used as separator]. <input style="width: 100px;" type="text" value="h#e#l#l#w#o#r#d#"/> Plaintext <input style="width: 100px;" type="text" value="helloworld"/>	
<div style="display: inline-block; width: 45%;">Encrypt</div> <div style="display: inline-block; width: 45%;">Decrypt</div> <div style="display: inline-block; width: 45%;">Close</div>		<div style="display: inline-block; width: 45%;">Encrypt</div> <div style="display: inline-block; width: 45%;">Decrypt</div> <div style="display: inline-block; width: 45%;">Close</div>	