|  |
| --- |
| RSA Algorithm:  Step 1. Choose two primes p and q.  Example: p = 3 and q = 11.  Step 2. Let n = p × q.  Example: n = 3 × 11 = 33.  Step 3. Let A = (p − 1)(q − 1).  Example: A = 2 × 10 = 20.  Step 4. Choose an integer E with 1 < E < A such that E and A have no common factors other than 1.  Example: Choose E = 7.  Step 5. Find the integer D with 1 < D < A such that D × E − 1 is a multiple of A. Example: As (3 × 7) − 1 = 20, we have D = 3.  The numbers n and E are the public key; they can be shared with anyone. The number  D is the private key; it must be kept secret.  How do we use it?  Lily wants to be able to receive a secret message from Frank. She sends him the values of n and E . It does not matter if this message is intercepted; the values of n and E can be made public. Only Lily knows the value of D.  When data is sent securely over the internet, it is protected by a system like this. Anyone can encrypt, but only the authorised recipient can decrypt. Let us see how to employ it.  Before a message can be encrypted, it must be converted into a number (or a sequence of numbers). The number must be less than n. Since n is so small in our example, we will assign distinct numbers (each less than n) to the letters of the alphabet, and encrypt our message one letter at a time.  Suppose the message is ‘HELP’. For simplicity, we suppose that the letters H, E, L and P were assigned the numbers 2, 3, 4 and 5, respectively.  H E L P 2 3 4 5  The next step is to raise each of these numbers to the power E = 7.  128 2187 16 384 78 125  Then find the remainders when each of these numbers is divided by n = 33. For example, we have 128 = 3 × 33 + 29, and so 128 gives a remainder of 29.  29 9 16 14  **The encrypted message to be sent is 29 9 16 14.**  The method for decryption is similar, but we use D instead of E . Start with the encrypted message.  29 9 16 14  Raise each number to the power D = 3.  24 389 729 4096 2744  Find the remainders when each number is divided by n = 33.  2 3 4 5  This is the original message. |