abstract :
Actualmente la criptografía clásica protege el intercambio de información, sin embargo los avances de la computación cuántica pone en peligro dicha protección,ya que, con los nuevos algoritmos cuánticos se ha demostrado que es posible vulnerar y romper muchos criptosistemas clásicos, ya sea asimétrico o simétrico. En este survey se mostrará diferentes técnicas que son usadas para resolver problemas como la factorización de número grandes, logaritmos discretos, y con un tiempo polinomial; con la finalidad de romper criptosistemas simétricos y asimétricos como DES (Data Encryption Standard) y RSA (Rivest, Shamir y Adleman).