**Caballero Huesca Carlos Eduardo.  3CV1**

Cifrado Vernam

Según el principio de Kerkhoff todos los algoritmos de cifrados y descifrados deben ser públicos y conocidos por todos, lo único secreto es la clave del algoritmo, esta clave se convierte en la piedra angular del algoritmo.
Basándose en este principio, el cifrado perfecto (el cifrado Vernam) debe ser público con su clave en secreto y ésta debe tener la misma longitud del mensaje, ser generada aleatoriamente y solamente puede ser usada una sóla vez.
Para cifrar el mensaje se realiza una operación XOR (or exclusivo) entre el mensaje y la clave.
Como se puede observar este método sería perfecto de no ser porque cada clave generada aleatoriamente debería ser generada también aleatoriamente e idéntica a la del emisor, por el receptor del mensaje, algo que en principio es muy díficil.

También se le conoce como “one time pad” o porque cada clave solo se puede usar una vez.
Efectivamente el problema es que como la clave es de un solo uso, tenemos que tener un montón de claves generadas cuando emisor y receptor estén juntos de manera que cada uno se lleve una copia, lo cual es muy incómodo.
Si el emisor del mensaje genera la clave en el momento de aplicar el cifrado, tendrá que enviar también la clave al receptor, para lo que necesitaría un canal seguro, pero en caso de tener un canal seguro, no necesita cifrado alguno,

La solución a este problema la plantea la mecánica cuántica  Gracias a la mecánica cuántica, podemos establecer un protocolo de manera que emisor y receptor (Alice y Bob) puedan tener la misma clave, generada en el momento, 100% aleatoria, estando ambos a distancia y además asegurándose de que nadie la ha copiado, pueden tener la certeza de que son los únicos que tienen esa clave. Gracias a este protocolo de generación/transmisión de clave, se puede usar el cifrado de Vernam sin los inconvenientes que plantea clásicamente.
Por cierto, según Shanon, “fundador” de la teoría de la información, este cifrado es el único 100% seguro que se conoce (siempre que la clave sea 100% aleatoria y se use una sola vez).