Criterios de Shannon

En los años cuarenta, Shannon sugirió los criterios básicos que debían cumplir
los sistemas de cifrado modernos. Los puntos a tener en cuenta eran:

a) El sistema debe proporcionar suficiente secreto.

b) El tamaño de la clave debe ser lo suficientemente corto para ser sencillo de recordar y lo suficientemente largo para proveer de suficiente seguridad.

c) Las operaciones de cifrado y descifrado deben ser sencillas.

d) El sistema debe tener una baja propagación de errores.

e) El tamaño del mensaje no debe crecer.

En el momento en que Shannon dio estas indicaciones, el uso de dispositivos electrónicos capaces de realizar de forma automática el cifrado era muy raro, costoso y en general no disponible para el uso público. Los sistemas de cifrado eran manuales y para ello era muy importante la simplicidad de uso. Evidentemente con la aparición de los ordenadores alguno de estos puntos no es tan relevante como en su día. Sin embargo en su base siguen siendo conceptos totalmente válidos en la actualidad.