ENCRYPTION FUNDAMENTALS - A NON-TECHNICAL OVERVIEW

Anthony Wechselberger

Oak Communications, Inc.

ABSTRACT

A popular buzzword today, "encryption" and its various spinoff terminology (cryptography, cryptanalysis, cypher...) are frequently used to bombard the observer attempting to understand an application into submission. Submission that the subject is just too esoteric for the average technocrat to understand; such that one just has to accept the "bombardier's" obfuscation.

This paper will explain in layman terminology the basics of encryption, as it's being applied in today's TV industry:

1. What is it?
2. Why do it?
3. What's special about it?
4. What are encryption algorithms, encryption keys?
5. Can it be misused, abused?
6. What questions should be asked about its application?
7. Why is it different from scrambling?
8. Why now?

The concepts of encryption and its proper application can be explained at a nontheoretical level. The paper will discuss the significance of digital versus analog coding for encryption applications, the many methods of using the encryption algorithm and why the algorithm (such as DES) does not represent the "strength" of an encryption system. The use of controlled access key variables as the most important problem to solve in any encryption application will be explained, and why, through solving that problem, encryption avoids the necessity for secrecy of circuits or physical security.