RESUMEN

Las radios definidas por *software* son una tecnología que actualmente se encuentra en desarrollo para el perfeccionamiento de las comunicaciones. Una de las partes más importantes de las comunicaciones es ocultar información para que no pueda ser intervenida e interpretada por personas ajenas a la misma, tomando en cuenta que se vive una era donde las comunicaciones digitales van reemplazando a grandes pasos los medios analógicos. La presente investigación pretende implementar algoritmos de cifrado en una radio definida por *software*, analizando diferentes sistemas criptográficos con el fin de proveer mayor seguridad a la radio. Utilizando los campos de Galois para varios medios, se desarrollaron códigos de cifrado que se adaptan a las características de seguridad deseadas para la implementación en las radios. Posteriormente se cuantificaron las pérdidas de datos en los diferentes modelos de radio simulados en función de la relación señal a ruido y la tasa de bit erróneos, además se usó como medida objetiva MBSD (del inglés *Modified Bark Spectral Distortion*). Finalmente se propone un modelo de radio que trabaja con las tarjetas USRP 2920 basado en el programa de LabVIEW®, con la aspiración de reemplazar los medios actuales de comunicación de las Fuerzas Armadas proveyéndolos de radios más seguras, más ligeras y con mayores prestaciones.

PALABRAS CLAVES:

- **CIFRADO**
- **ALGORITMOS**
- **CRIPTOGRAFÍA**

ABSTRACT

The Software Defined Radios are a technology that is currently in development for the improvement of communications. One of the most important parts of communications is to hide information so that it can not be intervened and interpreted by people outside of it, taking into account that there is an era where digital communications are replacing analogical media in a big way. The present research aims to implement encryption algorithms in a software-defined radio, analyzing different cryptographic systems in order to provide greater security to the radio. Using the Galois fields for various media, encryption codes were developed that adapt to the desired security features for the implementation in the radios. Subsequently, the data losses in the different simulated radio models were quantified as a function of the erroneous signal-to-noise ratio and bit rate, in addition it was used as objective measure MBSD (Modified Bark Spectral Distortion). Finally, a radio model that works with the USRP 2920 cards based on the LabVIEW® program is proposed, with the aspiration to replace the current means of communication of the Armed Forces by providing them with safer, lighter and higher performance radios.

KEYWORDS:

- **ENCRYPTION**
- **ALGORITHMS**
- **CRYPTOGRAPHY**