

# RAE

**Tipo de documento:** Tesis de Grado

**Acceso al documento:** Universidad Pedagógica Nacional

**Título del documento:** Encriptando información con dulces de colores, una simulación al protocolo BB84

**Autor(s):** REYES ROA, Yulieth Catherine

**Asesor:** Juan Manuel Rodríguez

**Publicación:** Bogotá, 2007, 66p

**Unidad Patrocinante:** Universidad Pedagógica Nacional

**Palabras Claves:** Clave, Código, Criptografía, Criptografía Cuántica, Protocolo, Protocolo BB84.

## DESCRIPCION DEL TRABAJO

Este trabajo da cuenta de la elaboración de un juego como herramienta pedagógica para dar a conocer el primer protocolo de Criptografía cuántica denominado protocolo BB84 en forma sencilla y dinámica, el cual se implementó en el colegio Magdalena Ortega de Nariño, en dos cursos del grado octavo durante la primera semana de Septiembre del 2007 y por medio del cual se obtuvieron los resultados y las conclusiones finales del trabajo.

## FUENTES

- [1] D. Bouwmeester, A. Ekert y A. Zeilinger. The physics of quantum computation. Springer Verlag (2000)
- [2] S. Singh. Los códigos secretos. Ed Debate S, A. Madrid (2000)
- [3] M. Dusek, N. Ludkenhaus, M. Hendrych. 2006. Quantum Cryptography. Los Alamos e-print archive: quant-ph /0601207
- [4] P. Caballero. Introducci3n a la criptograf3a. Madrid, Editorial Ra-ma, 2003.
- [5] C. Bennett, G. Brassard, A. Ekert. Criptograf3a cu3ntica .Rev. investigaci3n y ciencia. 195 (1992)
- [6] C. Williams, S. Clearwater, S. Telos. Explorations in quantum computing. The electronic library of Science. 1997
- [7] G. Stix. Rev.Criptograf3a cu3ntica comercial.investigaci3n y ciencia. 342 (2005) 8]J. Wiese. El super esp3a cient3fico. Mexico, Limusa, Wiley 2003

## CONTENIDO

El trabajo está dividido en 3 capítulos: El capítulo 1 recopila toda la información acerca de la criptografía en su contexto histórico, desde sus inicios, los métodos que se han desarrollado hasta el protocolo cuántico BB84. El segundo capítulo da a conocer el juego y las 3 misiones que lo conforman. Finalmente, en el capítulo 3 se describe la implementación del juego en el colegio Magdalena Ortega de Nariño con 2 cursos del grado octavo y los resultados obtenidos a través de la participación de las estudiantes dentro del juego, la solución que dieron a cada una de las misiones y las respuestas obtenidas en los dos cuestionarios que se llevaron al aula con el fin de identificar dificultades obtenidas dentro de la actividad y el conocimiento adquirido durante el desarrollo de la actividad.

## **METODOLOGIA**

Los pasos que se siguieron para la elaboración del trabajo fueron:

1. Recopilación de información
2. Diseño y elaboración del juego
3. Implementación del juego
4. Resultados y conclusiones del trabajo.

## **CONCLUSIONES**

Se logró recopilar información acerca de la criptografía y así mismo se investigó el tema a partir de las primeras formas de codificación hasta la criptografía cuántica, resaltando el planteamiento original del protocolo BB84 y sus características más representativas.

Se cumplió con el objetivo de diseñar un juego que simulara el protocolo BB84 en términos sencillos y se logró implementar en el aula ante una población estudiantil de octavo grado.

Se tomó el protocolo más sencillo para elaborar un juego dirigido a estudiantes de octavo grado y por medio de él se generó una participación activa por parte de las estudiantes facilitando la comprensión del tema.

Teniendo en cuenta los diferentes roles que tomaron las niñas dentro del juego (emisor, receptor y participantes) y los elementos que influyeron en el mismo (dulces y números binarios) se logró una buena interpretación del protocolo BB84 y se cumplió el objetivo de dar a conocer la criptografía cuántica.

El juego fue una buena herramienta para dar a conocer la QC porque a través de él las niñas se divertieron, adquirieron conocimiento, se cuestionaron, buscaron información por sí mismas y finalmente comprendieron el tema.

Por medio de las misiones, las niñas identificaron las diferencias entre la criptografía clásica y cuántica. Se puede elaborar un juego dirigido a estudiantes de física, que simule protocolos posteriores al BB84, tomando en cuenta el enredamiento cuántico, la paradoja ERP o los diferentes principios cuánticos que caractericen el protocolo a estudiar.

**Fecha de elaboración resumen:** 04 Diciembre del 2007