

**UNIVERSIDAD CIENTÍFICA DEL SUR**

**FACULTAD DE CIENCIAS DE INGENIERÍA Y EMPRESA**

**ESCUELA DE INGENIERÍA DE SISTEMAS EMPRESARIALES**

**Elaboración de un protocolo criptográfico de intercambio de clave simétrica que implemente cuatro servicios de seguridad tales como la confidencialidad, autenticación, verificación de integridad y no repudio con la finalidad de fortalecer la transmisión de información clasificada entre la Fuerza Aérea y el Comando Conjunto de las Fuerzas Armadas del Perú en favor de la lucha contra el Terrorismo y Narcotráfico.**

**Monografía para optar el Título de  
Ingeniero de Sistemas Empresariales**

**Luigui Aurelio Rivas Guevara**

**Miraflores, 2009**

# ÍNDICE GENERAL

<b>RESUMEN EJECUTIVO .....</b>	<b>1</b>
<b>EXECUTIVE RESUMEN .....</b>	<b>2</b>
<b>INTRODUCCION .....</b>	<b>5</b>
<b>CAPÍTULO 1.....</b>	<b>8</b>
<b>BASES CONCEPTUALES .....</b>	<b>8</b>
1.1 SEGURIDAD DE LA INFORMACIÓN.....	8
1.2 LA SEGURIDAD DE LA INFORMACIÓN EN LA INTERNET. ....	11
1.3 SERVICIOS DE SEGURIDAD DE LA INFORMACIÓN.....	12
<b>CAPITULO 2.....</b>	<b>15</b>
<b>EL MUNDO DE LA CRIPTOLOGÍA.....</b>	<b>16</b>
2.1 CRIPTOLOGÍA.....	17
2.1.1 Criptografía.....	17
2.1.2 Criptografía Simétrica o de Clave Secreta.....	18
2.1.3 Criptografía Asimétrica o de Clave Pública.....	19
2.1.4 Funciones Hash.....	21
<b>CAPÍTULO 3.....</b>	<b>23</b>
<b>PROTOCOLOS, ALGORITMOS Y APLICACIONES CRIPTOGRÁFICAS. ....</b>	<b>25</b>
3.1 DEFINICIÓN DE PROTOCOLO CRIPTOGRÁFICO.....	25
3.1.1 Tipos de Protocolos Criptográficos.....	26
3.1.2 Protocolos Criptográficos para implementar Servicios de Seguridad.....	28
3.1.3 Ejemplos de desarrollo de Protocolos Criptográficos.....	29
3.2 ALGORITMOS CRIPTOGRÁFICOS.....	34
3.2.1 Secure Hash Algorithm, Algoritmo de Hash Seguro (SHA).....	34
3.2.2 Algoritmo RSA.....	36
3.2.3 Algoritmo AES (Advanced Encryption Standard).....	38
3.3 APLICACIONES CRIPTOGRÁFICAS.....	40
3.3.1 Firma Digital .....	40
3.3.2 Certificados Digitales .....	42
3.4 LEGISLACIÓN EN EL PERÚ SOBRE EL USO DE APLICACIONES CRIPTOGRÁFICAS.....	43

<b>CAPITULO 4.....</b>	<b>44</b>
<b>DISEÑO DEL PROTOCOLO CRIPTOGRÁFICO.....</b>	<b>45</b>
4.1 DESARROLLO DEL PROTOCOLO CRIPTOGRÁFICO PROPUESTO.....	46
4.1.1 Definición del Objetivo, Suposiciones y Algoritmo Criptográficos a emplear. ....	46
<b>CAPITULO 5.....</b>	<b>54</b>
<b>CONCLUSIONES Y RECOMENDACIONES.....</b>	<b>54</b>

**BIBLIOGRAFIA**

**ANEXOS**