Cryptographer/Cryptanalyst

<table>
<tr><td><b>NICE Framework Reference</b></td><td colspan="2">None.</td></tr>
<tr><td><b>Functional Description</b></td><td colspan="2">Develops algorithms, ciphers, and security systems to encrypt information/Analyzes and decodes secret messages and coding systems.</td></tr>
<tr><td><b>Consequence of error or risk</b></td><td colspan="2">Error, neglect, outdated information or poor judgment could result in poor cryptologic artefacts, protocols, and systems that will jeopardize intended security of the systems / information they are protecting. Failure to keep up to date on related science and emerging technology carries equal risk.</td></tr>
<tr><td><b>Development pathway</b></td><td colspan="2">A highly specialized cybersecurity activity, this role is filled by experienced and educated professionals who are interested in this field. Opportunities exist for increased specialization and advanced research and studies in the field.</td></tr>
<tr><td><b>Other titles</b></td><td colspan="2">None.</td></tr>
<tr><td><b>Related NOCs</b></td><td colspan="2">2147 Computer engineers (except software engineers and designers)
2161 Mathematicians, statisticians and actuaries
2171 Information systems analysts and consultants</td></tr>
<tr><td><b>Tasks</b></td><td colspan="2">▪ Collaborate with key stakeholders to establish an effective cybersecurity risk management program
▪ Ensure compliance with the changing laws and applicable regulations
▪ Develop systems for protection of important/sensitive information from interception, copying, modification and/or deletion
▪ Evaluate, analyze and target weaknesses and vulnerabilities in security systems and algorithms
▪ Develop statistical and mathematical models to analyze data and troubleshoot security problems
▪ Develop and test computational models for reliability and accuracy
▪ Identify, research and test new cryptology theories and applications
▪ Decode cryptic messages and coding systems for the organization
▪ Develop and update methods for efficient handling of cryptic processes
▪ Prepare technical reports that document security processes or vulnerabilities
▪ Provide guidance to management and personnel on cryptical or mathematical methods and applications
▪ Support countermeasures and risk mitigation strategies against potential exploitations of vulnerabilities related to cryptographic systems and, algorithms
▪ Provide insights and guidance related to quantum safety and quantum resistant strategies
▪ Support incident management and post-analysis in the event of a compromise to encryption/cryptographic processes or systems
▪ Develop, deliver, and oversee related cybersecurity training material and educational efforts related to role
▪ Guide and support encryption specialists as required</td></tr>
<tr><td><b>Required qualifications</b></td><td>Education</td><td>Post-secondary university degree in Computer Engineering, Computer Science, or Mathematics. A Master of Science or Doctorate is preferred.</td></tr>
</table>

<table>
<tr><td></td><td>Training</td><td>As required to support organizational technical context (e.g. local tools, processes and procedures)</td></tr>
<tr><td></td><td>Work experience</td><td>In addition to academic credentials, entry level roles normally require 3-5 years’ experience in an IT/systems domain with familiarity of encryption and key management activities.</td></tr>
<tr><td><b>Tools &amp; Technology</b></td><td colspan="2">▪ Threat and risk assessments
▪ Vulnerability management processes and vulnerability assessments
▪ Incident management processes and procedures (crypto/encryption related)
▪ Cybersecurity risk management processes & policies
▪ Privacy and security legislation
▪ Cryptographic algorithms, ciphers and systems
▪ Key management policies and plans
▪ Organizational security infrastructure and reporting systems</td></tr>
<tr><td><b>Competencies</b></td><td colspan="2">Underpinning this occupation are those competencies demonstrated for an executive level which include those identified within the NICE framework.

Basic application of the following KSAs:
☐ Integrated/organizational security concepts, principles and practice (software, system, data, physical and personnel)
☐ Preventative technical, operational and management controls available and organizational responsibilities for those controls
☐ Sector/context relevant threats, business needs and technical infrastructure
☐ Information and data requirements including sensitivity, integrity and lifecycle
☐ Applicable computer programming languages
☐ Cybersecurity program management, measures and monitoring

Advanced application of the following KSAs:
☐ Advanced threats and crypto breaking /decryption capabilities
☐ Applicable laws, legal codes, regulations, policies and ethics as they relate to cybersecurity; and
☐ Computer architecture, data structures, and algorithms
☐ Linear/matrix algebra and/or discrete mathematics
☐ Probability theory, information theory, complexity theory and number theory
☐ Cryptography and cryptographic key management concepts;
☐ Principles of symmetric cryptography (e.g., symmetric encryption, hash functions, message authentication codes, etc.)
☐ Principles of asymmetric cryptography (asymmetric encryption, key exchange, digital signatures, etc.)
☐ Incident response requirements for cryptographic compromise
☐ Technical report writing</td></tr>
<tr><td><b>Future Trends Affecting Key Competencies</b></td><td colspan="2">▪ The increased reliance on virtualized and/or ‘cloud-based’ services will require knowledge of responsibilities of the services provider including their cybersecurity responsibilities relative to organizational cybersecurity risks particularly as they pertain to data encryption requirements.
▪ Increased use of automated tools, aided by artificial intelligence, will require understanding of how the cryptographic tools are affected and automated to support organizational requirements.</td></tr>
</table>

	▪ Increased use of automated tools by threat actors pose challenges for organizations that do not have complementary defensive tools to ensure robust cryptographic systems, ciphers and algorithms. If there are known disparities between the threat and the ability to defend, mitigations should be defined and implemented ▪ Mechanisms to support the required level of trust and organizational risk will need to be in place to support monitoring and reporting of results from automated tools. Consequently, there will be a need to understand organizational risks posed, measures of security and what policies, processes, or procedures need to be in place. ▪ The emergence and use of quantum technologies by threat actors will fundamentally change encryption security. This will require knowledge and skills related to implementing a quantum safe strategy within the organization. The cryptographer/cryptanalyst will play a key role in ensuring quantum safe/resistant design and may be involved in testing of algorithms, encryption protocols and equipment.