



AVIS DE RECRUTEMENT

Type de contrat : **CDD 02 ans**

Disponibilité immédiate

INGENIEUR CRYPTOLOGUE (H/F)	
Employeur	Agence des Systèmes d'Information et du Numérique (ASIN)
Superviseur Hiérarchique	Responsable Service Chiffres
Entité	Pôle Sécurité Numérique/Département Cybersécurité
Relation fonctionnelle	Tous directeurs et autres collaborateurs
Lieu d'affectation	Cotonou
Candidature	Postuler en ligne sur le portail national des services publics https://servicepublic.bj/public/services/service/PS01334 en joignant un CV actualisé, une lettre de motivation, la copie des diplômes et une pièce d'identité au plus tard le 19 octobre 2026 à 20h00 (heure de Cotonou).

INFORMATIONS GENERALES

La République du Bénin a lancé un programme ambitieux de développement de l'économie numérique visant à positionner le pays comme la référence en matière de plateforme de services numériques en Afrique de l'Ouest et de faire des Technologies de l'Information et de la Communication le principal levier de son développement socio-économique.

L'Agence des Systèmes d'Information et du Numérique (ASIN) est une agence gouvernementale sous la double tutelle du Ministère de l'Économie et des Finances et du Ministère de la Transformation Digitale et de l'Innovation, chargée d'assurer la mise en œuvre opérationnelle des programmes et projets entrant dans le cadre des stratégies de développement des services et systèmes d'information sécurisés au Bénin. À ce titre, elle conçoit, déploie et maintient les plateformes nationales de services publics numériques, les référentiels et les briques d'interopérabilité qui permettent aux administrations d'échanger leurs données et de servir les usagers de manière simple, sécurisée et continue.

CONTEXTE ET PORTEE DE LA MISSION DU POSTE

Sous la responsabilité du Chef service Chiffres, l'ingénieur cryptologue participe à l'opérationnalisation de la Commission Cryptologie. Il/Elle apporte une expertise technique et réglementaire à la Commission Cryptologie. Il/Elle contribuera aux activités du service en termes de formation et sensibilisation.

PRINCIPALES RESPONSABILITES

- Instruire les dossiers de déclaration d'importation, d'exportation et d'agrément des prestataires de services de cryptologie ;
- Réaliser les analyses techniques des moyens de cryptologie soumis à la Commission ;



- Évaluer la conformité réglementaire des solutions cryptographiques proposées par les opérateurs
- Participer aux travaux de la Commission Cryptologie et préparer les rapports techniques destinés aux membres de la Commission
- Élaborer les procédures d'instruction, d'évaluation et de contrôle des activités de cryptologie
- Contribuer à la rédaction des textes réglementaires, guides techniques et référentiels nationaux en matière de cryptologie
- Conduire des audits techniques des dispositifs cryptographiques utilisés par les organismes publics et les opérateurs soumis au Code du Numérique
- Participer aux inspections et aux missions de contrôle prévues par les textes réglementaires
- Assurer une veille scientifique, technologique et réglementaire sur les technologies cryptographiques, et les normes internationales
- Contribuer au développement des capacités nationales en cryptographie par la formation des administrations, des entreprises et des membres de la Commission
- Participer aux projets nationaux impliquant les infrastructures à clés publiques (PKI) la signature électronique, le chiffrement gouvernemental et les infrastructures critiques
- Produire des rapports d'expertise et des avis techniques destinés aux autorités compétentes
- Exécuter toutes autres tâches confiées par le supérieur.

FORMATION, EXPÉRIENCE ET LANGUES

FORMATION

Être titulaire d'un diplôme Bac+5 minimum (Master ou diplôme d'ingénieur) en Cryptologie, Cryptographie et informatique, Sécurité des SI ou Cybersécurité, Mathématiques appliquées à la cryptologie ou tout autre domaine équivalent.

EXPERIENCE

- Trois (03) années dans le domaine de la sécurité des systèmes d'information
- Une solide expérience dans la conception et l'évaluation des primitives et protocoles cryptographiques ; la mise en œuvre des infrastructures à clés publiques (PKI), des modules de sécurité matériel (HSM), gestion de clés cryptographiques, signature électronique ou système équivalent
- Une solide expérience en audit de sécurité ou en conformité réglementaire
- Une certification ECES, CISA, ISO 27001 LA, CHFI, CEH, serait un atout.

LANGUES

- Une excellente maîtrise de la langue française, aussi bien à l'oral qu'à l'écrit, est exigée
- Une bonne maîtrise de l'anglais dans un contexte professionnel est requise.

CONNAISSANCES ET COMPETENCES

Connaissances requises

- *Normes internationales* : ISO/IEC 27001 ; ISO/IEC 27002 ; ISO/IEC 19790 ; ISO/IEC 15408 (Common Criteria) ; ETSI Electronic Signature Standards ; RFC de l'IETF relatifs à la cryptographie et aux infrastructures PKI



- Une excellente connaissance des publications et standards du National Institute of Standards and Technology (NIST) est fortement souhaitée, notamment ;
- Développement sécurisé ;
- Compréhension des architectures x86/x64, ARM et RISC-V ;
- Analyse des exécutables Windows (PE), Linux (ELF) et macOS (Mach-O) ;
- Maîtrise du langage assembleur (x86/x64, ARM) ;
- Développement d'outils d'analyse en Python, C/C++, Rust, Go, Java ;
- Maîtrise des plateformes et technologies web sécurisés, des protocoles cryptographiques (TLS, SSH) et bibliothèques cryptographiques (OpenSSL, LibreSSL, Bouncy Castle, Libsodium, BoringSSL, ...).

Compétences requises

➤ **Cryptographie :**

- Cryptographie classique (AES, RSA, ECC, PKI, Chiffrement homomorphe, etc.) ;
- Cryptographie légère (Ascon, ACORN, PRESENT, GIFT, SKINNY, TinyJAMBU, etc.) ;
- Cryptographie post-quantique (Isogénie sur les courbes elliptiques, réseaux euclidiens, ML-KEM, ML-DSA, SLH-DSA, FN-DSA, etc.)
- Cryptographie quantique (BB84, Qubits, QKD, QRNG, réseaux quantiques, Internet quantique, etc.) ;
- Fonctions de hachage (SHA-2, SHA-3, SHAKE, BLAKE2, fonctions éponges, MAC, etc.) ;
- Technologies blockchain et l'intelligence artificielle.

➤ **Cryptanalyse :**

- Cryptanalyse classique, différentielle, linéaire, algébrique ;
- Cryptanalyse différentielle et linéaire avancée, par injection de fautes ;
- Cryptanalyse des implémentations, des générateurs aléatoires, des fonctions de hachage, des cryptosystèmes asymétriques.
- Analyse des implémentations cryptographiques ;
- Audit des produits cryptographiques ;
- Identification, compréhension et évaluation des implémentations cryptographiques propriétaires ou commerciales ;
- Analyse des protocoles de communication et des formats de données propriétaires ;
- Recherche de vulnérabilités dans les implémentations cryptographiques ;
- Évaluation de la robustesse des mécanismes de protection des clés cryptographiques
- Analyse de malwares intégrant des mécanismes cryptographiques.

ETHIQUE, MANAGEMENT ET LEADERSHIP

- Rigueur, esprit de synthèse et d'analyse ;
- Capacité à travailler de manière autonome ;



- Excellente capacité rédactionnelle (Rédaction de rapports d'analyse technique et de preuves de concept (PoC).
- Capacité d'écoute et communication orale et écrite ;
- Capacité à gérer le temps, les priorités, et à répondre aux changements des priorités (flexibilité) ;
- Capacité à représenter l'ASIN auprès des instances nationales et internationales relatives à la cryptologie ;
- Sens aigu de l'éthique, de la transparence, de l'intégrité et de la confidentialité ;
- Sens du travail en équipe.