



PREMIER MINISTRE

Secrétariat général
de la défense nationale

Agence nationale de la sécurité
des systèmes d'information

FICHE de POSTE

L'agence nationale de la sécurité des systèmes d'information recherche un

Spécialiste en protocoles cryptographiques

- Rattachement** : Secrétariat général de la défense nationale (SGDN)
Agence nationale de la sécurité des systèmes d'information (ANSSI)
Laboratoire Cryptographie et Composants (LCC)
- Lieu de travail** : Hôtel national des Invalides, 51 boulevard de La Tour-Maubourg (Paris 7^e)
et locaux techniques du laboratoire au 120 rue du Cherche-Midi (Paris 7^e)
- Type de contrat** : Contrat à durée déterminée (CDD) de 3 ans renouvelable
- Disponibilité** : Poste à pourvoir immédiatement
- Rémunération** : Selon compétence et expérience

Environnement

L'agence nationale de la sécurité des systèmes d'information ([ANSSI](#)) appartient au secrétariat général de la défense nationale ([SGDN](#)), service du Premier ministre chargé d'assister le chef du Gouvernement dans l'exercice de ses responsabilités en matière de défense nationale et de sécurité nationale.

L'action de l'ANSSI a pour objectif d'assurer la sécurité des systèmes d'information de l'Etat et des opérateurs nationaux d'importance vitale, de concevoir et de déployer les réseaux sécurisés répondant aux besoins des hautes autorités de l'Etat et aux besoins interministériels, et de créer les conditions d'un environnement de confiance et de sécurité propice au développement de la société de l'information en France et en Europe.

Le laboratoire « Cryptographie et Composants » est le pôle d'expertise de l'ANSSI dans les domaines de la cryptographie et des composants cryptographiques. Il participe notamment, dans ces domaines, à la recherche, à l'analyse des besoins et à la conception des solutions propres à les satisfaire, à l'évaluation des produits et à l'élaboration et à la mise à jour de référentiels techniques.

Activités principales

Cet ingénieur aura la charge de contribuer aux travaux d'expertise et de recherche et développement menés dans le domaine des protocoles cryptographiques. Il sera chargé d'analyser la sécurité de protocoles cryptographiques et de leur implémentation dans le but de les voir ensuite intégrés dans des composants de sécurité. Il assurera, par des activités de recherche, le suivi de l'état de l'art et des vulnérabilités éventuelles liées à son domaine d'activité, en particulier dans le domaine de la cryptographie à clé publique et des preuves de sécurité. Il apportera son expertise technique dans les travaux d'évaluation des compétences des centres d'évaluation de la sécurité des technologies de l'information (CESTI) en vue de leur agrément par l'ANSSI. Il contribuera aux travaux techniques internationaux au sein de l'Union Européenne et de l'OTAN dans le domaine de la mise en œuvre des protocoles cryptographiques afin d'en assurer la cohérence avec le cadre national. Enfin il contribuera au

développement de produits de sécurité robustes par l'analyse des mécanismes cryptographiques soumis aux processus d'évaluation de l'ANSSI, par l'élaboration et le maintien à jour d'un référentiel fixant les règles et les recommandations à respecter pour les produits de sécurité employant des mécanismes cryptographiques, et par une activité de conseil et d'assistance auprès des acteurs majeurs du domaine.

Compétences et expérience

Le titulaire devra être titulaire d'une thèse de doctorat dans le domaine de la cryptographie. Il devra justifier d'une activité de recherche ou d'expertise dans le domaine des protocoles cryptographiques ou des preuves de sécurité. Des connaissances dans le domaine de la cryptographie sur courbes elliptiques seraient également appréciées.

Compétences mises en œuvre

- Cryptographie, analyse de protocoles cryptographiques, élaboration et vérification de preuves de sécurité, expertise en sécurité de mécanismes cryptographiques
- Algorithmique, programmation
- Connaissances en géométrie des nombres (courbes elliptiques et hyperelliptiques)
- Pratique courante de l'anglais, écrit et oral
- Expérience pratique de mise en œuvre de protocoles cryptographiques

Qualités requises

- Esprit d'initiative
- Autonomie
- Rigueur et esprit de synthèse
- Capacité d'adaptation et de travail en équipe
- Capacité à restituer clairement une analyse à des interlocuteurs variés (experts ou non)

Habilitation

Le poste nécessite un accès au secret de défense nationale. Une procédure d'habilitation sera conduite dans ce but au niveau Secret Défense (conformément à l'IGI 1300 SGDN/PSE).

Contact

Les candidatures sont à adresser :

- de préférence, par courrier électronique :
secretariat.anssi@ssi.gouv.fr
- ou par courrier postal :

Agence nationale de la sécurité des systèmes d'information
51, boulevard de La Tour Maubourg
75700 Paris 07 SP

Des compléments d'information peuvent être demandés par courrier électronique à :

crypto.dcssi@sgdn.gouv.fr