



Offre n°2024-08402

Ingénieur scientifique contractuel / Cryptographie historique

Type de contrat : CDD

Niveau de diplôme exigé : Bac + 5 ou équivalent

Fonction : Ingénieur scientifique contractuel

Niveau d'expérience souhaité : De 3 à 5 ans

Contexte et atouts du poste

Dans le cadre d'un partenariat

- collaboration entre 2 équipes Inria : Caramba (cryptographie à Nancy), et Almanach (IA à Paris)
- action exploratoire **Back In Time**, dont le but est de mettre en collaboration trois domaines d'expertise différents (histoire, cryptographie, intelligence artificielle) pour développer, à terme, un logiciel libre capable de transcrire puis décrypter des lettres manuscrites chiffrées. L'attention se portera d'abord sur des documents du XVI^e au XIX^e siècle.

L'objectif de ce poste est de réfléchir et développer, d'abord un prototype, puis un module qui s'intégrera à une infrastructure plus grosse et déjà existante (Transkribus), particulièrement dédié au décryptage de documents chiffrés historiques.

Des déplacements sont possibles pour ce poste, d'une part pour rencontrer et collaborer avec la branche IA du projet Back In Time, qui se situe à Paris et à Lyon, d'autre part pour s'initier aux archives et pour diffuser nos résultats en conférence. Dans tous les cas, cela sera décidé en concertation avec l'ingénieur et les frais de déplacements seront pris en charge dans la limite du barème en vigueur.

Mission confiée

Missions :

Le coeur du projet consiste à la compréhension des méthodes de chiffrement homophoniques et à registre et à l'élaboration de méthodes de décryptage adéquates. Aussi étonnant que cela puisse paraître, les méthodes de décryptage historique qui existaient très probablement ne sont pas parvenues jusqu'à nous. L'ingénieur pourra se renseigner à ce sujet grâce à l'expertise bienvenue de l'historienne qui travaille dans notre équipe.

L'idée sera donc de mettre en place des algorithmes de décryptage performants, en s'inspirant des techniques existantes. En effet, les algorithmes d'optimisation de type hill climbing ou recuit simulé donnent des premiers résultats encourageants. Avec l'aide des chercheurs en cryptographie de l'équipe Caramba, la personne recrutée sera amenée à développer ces algorithmes de décryptage. Le premier corpus d'étude sera la correspondance manuscrite de l'un des ambassadeurs de l'empereur Charles Quint (XVI^e siècle). Cette correspondance représente des centaines de pages chiffrées et nous offre un jeu de test grande nature. D'autres chiffrements d'autres auteurs et d'autres époques seront par la suite envisagés, notamment des lettres ultramarines du XVIII^e siècle ayant pour décor la guerre d'indépendance des Etats-Unis.

Collaboration :

La personne recrutée sera en lien avec les deux ingénieurs contractuels de l'action exploratoire Back In Time, qui travaillent à Paris pour la partie intelligence artificielle et transcription du projet. Elle collaborera en cryptographie avec les membres du projet dans l'équipe Caramba à Nancy (Pierrick Gaudry, Paul Zimmermann, Cécile Pierrot) et pourra travailler également avec l'historienne en délégation dans notre équipe (Camille Desenclos).

Responsabilités :

La personne recrutée a la charge du développement du module de cryptographie qui s'intégrera à Transkribus ; il ou elle prendra des initiatives pour la création et l'amélioration de ce module.

Principales activités

Principales activités :

- Analyser les algorithmes de décryptage historique existants
- Proposer des solutions pour le décryptage des chiffrements homophoniques et des chiffrements à registre

- Prendre en main le prototype existant et développer un programme fonctionnel
- Intégrer les algorithmes de décryptage dans une infrastructure plus grande, à la suite des méthodes de transcription

Activités complémentaires :

- Rédiger la documentation explicative des algorithmes développés
- Contribuer à la rédaction d'articles scientifiques pour la diffusion des résultats
- Présenter l'avancée des travaux en interne (avec nos collaborateurs de Caramba et d'Almanach) et en conférence
- Contribuer à l'analyse des documents d'archive (initiation)

Compétences

Compétences techniques et niveau requis : Bac + 5 en informatique, expérience en développement et/ou de travail dans un cadre académique de 3 ans minimum

Langues : anglais de travail (impératif, les documents fournis seront en anglais). Si le collaborateur est à l'aise en français, le français sera aussi possible comme langue de travail. La langue de rédaction des articles de recherche éventuel sera l'anglais.

Compétences additionnelles appréciées : nous sommes sur un projet interdisciplinaire, donc de la curiosité pour les autres disciplines rendra le poste plus agréable pour le ou la candidat(e) !

Avantages

- Restauration subventionnée
- Transports publics remboursés partiellement
- Congés: 7 semaines de congés annuels + 10 jours de RTT (base temps plein) + possibilité d'autorisations d'absence exceptionnelle (ex : enfants malades, déménagement)
- Possibilité de télétravail (après 6 mois d'ancienneté) et aménagement du temps de travail
- Équipements professionnels à disposition (visioconférence, prêts de matériels informatiques, etc.)
- Prestations sociales, culturelles et sportives (Association de gestion des œuvres sociales d'Inria)
- Accès à la formation professionnelle
- Sécurité sociale

Rémunération

A partir de 2692 € brut/mois selon expérience et diplômes

Informations générales

- **Thème/Domaine** : Algorithmique, calcul formel et cryptologie
Ingénierie logicielle (BAP E)
- **Ville** : Villers lès Nancy
- **Centre Inria** : [Centre Inria de l'Université de Lorraine](#)
- **Date de prise de fonction souhaitée** : 2025-02-01
- **Durée de contrat** : 12 mois
- **Date limite pour postuler** : 2025-01-05

Contacts

- **Équipe Inria** : [CARAMBA](#)
- **Recruteur** :
Pierrot Cécile / cecile.pierrot@inria.fr

A propos d'Inria

Inria est l'institut national de recherche dédié aux sciences et technologies du numérique. Il emploie 2600 personnes. Ses 215 équipes-projets agiles, en général communes avec des partenaires académiques, impliquent plus de 3900 scientifiques pour relever les défis du numérique, souvent à l'interface d'autres disciplines. L'institut fait appel à de nombreux talents dans plus d'une quarantaine de métiers différents. 900 personnels d'appui à la recherche et à l'innovation contribuent à faire émerger et grandir des projets scientifiques ou entrepreneuriaux qui impactent le monde. Inria travaille avec de nombreuses entreprises et a accompagné la création de plus de 200 start-up. L'institut s'efforce ainsi de répondre aux enjeux de la transformation numérique de la science, de la société et de l'économie.

L'essentiel pour réussir

Le ou la collaborateur(trice) attendu(e) devra se reconnaître dans les éléments suivants :

- appétence pour le sciences
- curiosité pour l'histoire (aucun prérequis n'est demandé en histoire)

- excellent niveau en développement
- maîtrise du Python et du C
- compétences et familiarité d'autres langages informatiques bienvenues
- connaissances en cryptographie bienvenues, mais non indispensables
- se sentir à l'aise dans un environnement de dynamique scientifique, multiculturel

Attention: Les candidatures doivent être déposées en ligne sur le site Inria. Le traitement des candidatures adressées par d'autres canaux n'est pas garanti.

Consignes pour postuler

Sécurité défense :

Ce poste est susceptible d'être affecté dans une zone à régime restrictif (ZRR), telle que définie dans le décret n°2011-1425 relatif à la protection du potentiel scientifique et technique de la nation (PPST). L'autorisation d'accès à une zone est délivrée par le chef d'établissement, après avis ministériel favorable, tel que défini dans l'arrêté du 03 juillet 2012, relatif à la PPST. Un avis ministériel défavorable pour un poste affecté dans une ZRR aurait pour conséquence l'annulation du recrutement.

Politique de recrutement :

Dans le cadre de sa politique diversité, tous les postes Inria sont accessibles aux personnes en situation de handicap.