Curriculum vitae

BRICE CANVEL

Né le 21 juillet 1975 à Nantes – Nationalité française –
Permis d'établissement C – Célibataire

Enseignant en mathématiques et informatique au Collège Sainte Croix à Fribourg

Ingénieur en informatique

Expérience professionnelle

Depuis Sept. 2009 **Enseignant en mathématiques et informatique**
Collège Sainte Croix, Fribourg, Suisse

Sept. 2008 - Juin 2009 **Enseignant stagiaire en mathématiques et informatique**
Gymnase Intercantonal de la Broye, Payerne, Suisse

Juin 2003 - Août 2008 **Ingénieur sénior en développement de logiciels pour cartes à puce**
NagraCard S.A., Groupe Kudelski, Cheseaux-sur-Lausanne, Suisse

- Gestion de projets et gestion d'équipes.
- Formation des nouveaux ingénieurs dans le domaine de la cryptographie et des systèmes d'accès conditionnels utilisés pour la télévision payante.
- Développement de logiciel sur carte à puce. En particulier développement d'algorithmes de cryptographie et étude des aspects plus généraux de la sécurité sur les cartes à puce.

Févr. 2002 – Avr. 2003 **Assistant chercheur en cryptographie et sécurité informatique**
Laboratoire de Sécurité et de Cryptographie, EPF Lausanne, Suisse

- Participation à l'enseignement d'un cours de sécurité des réseaux destiné à des étudiants de 4ème et 5ème années.
- Étude du protocole SSL, utilisé pour sécuriser les communications sur Internet.
- Encadrement d'un projet étudiant dans le domaine des attaques de type analyse de courant sur des cartes à puce.

Févr. 2000 - Déc. 2001 **Ingénieur recherche et développement spécialisé en cryptographie et en sécurité**
Atmel Smartcard ICs, East Kilbride, Ecosse

- Développement de systèmes d'exploitation pour cartes à puce.
- Évaluations sécuritaires sur les cartes à puces.

Formation

Sept. 2008 - Juin 2009 **Diplôme d'aptitude à l'enseignement secondaire II (DAES II) en mathématiques et informatique**
Université de Fribourg, Suisse

Oct. 1998 – Sept. 1999 **Master of Science (MSc) en analyse numérique et informatique**
(mention «distinction»)
Université de Manchester, Angleterre

- Projet de fin d'études de 5 mois sur les attaques de type analyse de courant sur des cartes à puce, appliquées à l'algorithme de chiffrement à clé publique RSA.
- Participation à l'enseignement de Matlab destiné aux étudiants de 2ème année.
- Participations à l'enseignement d'un cours d'analyse destiné aux étudiants de 1ère année.

Oct. 1994 - Juill. 1998 **Bachelor of Science (BSc) en mathématiques et informatique**
Université de Strathclyde, Glasgow, Ecosse

- Projet de fin d'études sur l'algorithme de chiffrement à clé publique RSA et la factorisation par l'algorithme du crible quadratique.

Publications scientifiques

Août 2003 B. Canvel, A. Hiltgen, S.Vaudenay, M. Vuagnoux,
Password Interception in a SSL/TLS Channel,
CRYPTO '03, 17-21 août 2003, Santa Barbara, USA

Divers

Langues	Français	langue maternelle
	Anglais	courant et technique (Cambridge Proficiency Exam)
	Allemand	moyen

Permis de conduire voiture

Loisirs Sports (tae kwondo, course à pied, sports de montagne),
Guitare, Voyages à vélo

Lausanne, le 3 mai 2009