

Cette note décrit les principales caractéristiques de la librairie de calcul RSA à exposant public de Spirtech.

D'autres librairies cryptographiques (hash SHA-1, RIPE-MD, MD5, contrôle de signature ISO/IEC 9796-2, PKCS#1, MPE V5.2...) sont également disponibles.

Présentation

La librairie RSA Spirtech effectue le calcul de $(a^e \text{ mod } n)$ nécessaire dans les cryptosystèmes de RSA et Rabin, pour l'exposant public.e. Elle est particulièrement bien adaptée au contrôle des signatures RSA, par exemple pour s'assurer de l'intégrité d'un logiciel téléchargé, ou de la validité d'une carte à puce.

La librairie a été testée dans de nombreux environnements, et est utilisée par plusieurs grands fabricants de terminaux de paiements bancaires et cartes à puce. Un jeu de test spécialement développé par Spirtech en garantit un fonctionnement sûr dans tous les cas de figure après portage sur un nouvel environnement.

Elle a été particulièrement optimisée afin de respecter des durées d'exécution compatibles avec une utilisation dans des environnements à microcontrôleur peu ou moyennement puissants.

Performances

Voici un exemple des performances de notre librairie :

Contrôle d'une "Valeur d'Authentification" (VA/VS) ou signature, pour e=3.

CPU	Horloge	320 bits	512 bits	768 bits	896 bits	1024 bits	1152 bits	2048 bits
68HC11	6 MHz (Eclk)	0,041 s	0,10 s	0,23 s	0,31 s	0,40 s	0,51 s	1,60 s
80C51	33 MHz (Xtal)	0,057 s	0,14 s	0,32 s	0,44 s	0,57 s	0,72 s	2,26 s

Principales caractéristiques techniques

- Conforme aux spécifications MPE V5.2 et EMV2000.
- Taille et format de clé totalement flexible, jusqu'à 2048 bits.
- Exposant e de 2 à $2^{32}-1$.
- Interface C ANSI très simple, masquant la complexité interne de l'algorithme.
- Contrôle des paramètres entrants à chaque exécution.
- Portable (chaînes de développement Keil, IAR, Introl...).
- Taille RAM et code minime (0,8 ko RAM résultat compris, 1,2 ko code).
- Licence : 30 k€ ; transféré sous forme de logiciels source, sans royalties sur l'exécutable.
- Livrée avec documentation, exemples, et programme de validation complet.

Nous consulter pour d'autres microprocesseurs et environnements.

Spirtech

Spirtech est une jeune société, essaimage du laboratoire technique du Groupe Innovatron, spécialiste de la cryptographie et de la carte à mémoire.

Spirtech réalise des logiciels cryptographiques et des logiciels pour cartes à puce et modules de sécurité. Spirtech effectue également des spécifications de gestion de clés cryptographiques et des spécifications de systèmes utilisant des cartes à puce, sans ou avec contacts.

Nous réalisons par exemple les spécifications des systèmes télé billettiques Icare (CD97) pour la RATP et la SNCF, ainsi que l'architecture sécuritaire de gestion des modules de sécurité et de clés cryptographiques pour la généralisation de la télé billettique en Ile de France.

Pour tous renseignements complémentaires, vous pouvez contacter François GRIEU, directeur technique de Spirtech, au +33 1 40 46 36 22 (email : francois.grieu@spirtech.com).