COURS ID12 « INTRODUCTION À LA CRYPTOLOGIE »
COURS 8
LA CRYPTOGRAPHIE DANS LA "VRAIE VIE" : NORMES, STANDARDS, LOIS, IMPLANTATIONS.

PAUL ZIMMERMANN

1.1. **Les brevets historiques.** Les premiers brevets datent de 1976.

Inventeurs	Brevet	Date	Objet
Ehrsam et al.	3.962.539	8 juin 1976	DES
Hellman, Diffie, Merkle	4.200.770	29 avril 1980	échange de clé D.-H.
Hellman, Merkle	4.218.582	19 août 1980	systèmes à clé publique
Rivest, Shamir, Adleman	4.405.829	20 sept. 1983	RSA

Les brevets américains ont une durée de 17 ans. Donc RSA est dans le domaine public depuis septembre 2000.

1.2. **Brevets plus récents.**

Inventeurs	Brevet	Date	Objet
Shamir, Fiat	4.748.668	31 mai 1988	authent. F.-S.
Brachtl et al.	4.908.861	13 mars 1990	MDC-2, MDC-4
Schnorr	4.995.082	19 février 1991	signature Schnorr
Guillou, Quisquater	5.140.634	18 août 1992	authent. G.-Q.
Kravitz	5.231.668	27 juillet 1993	signature DSA
Micali	5.276.737	4 janvier 1994	*fair cryptosystems*

1.3. **Brevets connexes.**

Inventeurs	Brevet	Date	Objet
Massey, Omura	4.567.600	28 janvier 1986	arith. base normale
Hellman, Bach	4.633.036	30 décembre 1986	gén. premiers forts
Merkle	4.881.264	14 novembre 1989	*one-time signature*
Brickell et al.	5.299.262	29 mars 1994	exponentiation

Voir `http://www.micropatent.com` pour les nouveaux brevets (code 380 pour la cryptographie).

2. Les standards

2.1. **Standards internationaux (ISO et IEC).** ISO = *International Organization for Standardization*; IEC = *International Electrotechnical Commission*. Chaque standard est revu tous les 5 ans : prolongé, modifié, ou supprimé.

Date: `zimmerma@loria.fr`.

8372	modes pour chiffrement par bloc (ECB, CBC, CFB, OFB)
9796	signature à recrouvrement de message
9797	MAC = *message authentication code*
9979	registre d'algorithmes cryptographiques
10118-1...4	fonctions de hachage
11770-1...3	gestion de clé
13888-1...3	non répudiation
14888-1...3	signature à appendice

Aussi : nouveau standard AES (*Advanced Encryption Standard*) qui remplace DES. Choix de Rijndael parmi 15 puis 5 algorithmes, développé en Belgique par l'équipe de Bart Preneel (Joan Daemen et Vincent Rijmen) à Louvain. Octobre 2000 : annonce du choix du NIST. Les propositions devaient être faites pour le 12 septembre 1997, avec des clés de 128, 192, et 256 bits. Cf `http://csrc.nist.gov/encryption/aes/` et `http://www.esat.kuleuven.ac.be/~rijmen/rijndael/`. Rijndael peut avoir des tailles de clé et de bloc arbitraires, multiples de 32 bits.

2.2. **Standards bancaires.** ANSI = *American National Standards Institute*. On distingue les transactions courantes (*retail* ou R, moyenne 50 dollars par transaction) des transactions banque à banque (*wholesale* ou W, moyenne 3 millions de dollars par transaction). Standards ANSI :

X3.92	data encryption algorithm (DEA)
X9.9	authentification de message (W)
X9.17	gestion de clé (W)
X9.23	chiffrement (W)
X9.30-1	signature digitale (DSA)
X9.31-1	signature digitale (RSA)
X9.42	gestion de clé à la Diffie-Hellman
X9.52	triple DES
X9.57	gestion de certificat

Standards ISO :

8730	authentification de message
10126	chiffrement de message (W)
11166	gestion de clé

2.3. **Standards américains.** FIPS = *Federal Information Processing Standard*

46-2	DES
112	password
113	CBC-MAC
180-1	SHA-1
186	DSA
196	*entity authentification (asymmetric)*
197	AES

2.4. **Standards Internet.** RFC = *Request for Comments*

1319	fonction de hachage MD2
1421-1424	mail : chiffrement, gestion clé, certification
1510	Kerberos
1828	MD5 avec clé
1847-1848	sécurité sous MIME
1938	*one-time password*

Pour en savoir plus :

– standards FIPS : *Computer Security Resource Center* `http://csrc.ncsl.nist.gov/`
– RFCs : *Internet Network Information Center* `http://www.internic.net/` et *Internet Engineering Task Force* `http://www.ietf.org/`

3. Tailles de clé recommandées

Cf table de Lenstra et Verheul (`http://security.ece.orst.edu/koc/ece575/papers/cryptosizes.pdf`).

Voir aussi *ECRYPT Yearly Report on Algorithms and Key Lengths* (`http://www.ecrypt.eu.org/documents/D.SPA.10-1.1.pdf`).

	Block Cipher	RSA	Elliptic Curve	DSA
Export Grade	56	512	112	512/112
Traditional	80	1024	160	1024/160
Recommended	112	2048	224	2048/224
LV 2000	70	952	132	952/125
LV 2010	78	1369	146/160	1369/138

4. Législation

4.1. **Accords de Wassenaar.** Signés en 1996 par 31 pays, pour le contrôle de l'exportation d'armes et de procédés à usage militaire et civil comme la cryptographie.

Libre d'exportation : jusqu'à 56 bits pour clé secrète, jusqu'à 512 bits pour la clé publique, et jusqu'à 112 bits pour les algorithmes basés sur des calculs dans des sous-groupes (en particulier les courbes elliptiques).

Libre pour le marché de masse : crypto à clé secrète jusqu'à 64 bits (limite supprimée le 1er décembre 2000).

L'exportation de procédés protégeant la propriété intellectuelle est libre (par exemple DVDs).

Pour tout le reste, il faut une licence d'exportation.

4.2. **En France.** Voir l'interview d'un avocat sur `http://www.juriscom.net/pro/1/crypto3.htm`.

L'importation de produits hors CE, et l'exportation dépend de la loi du 26 juillet 1996, et des décrets d'application du 24 février 1998 et du 17 mars 1999 : pas besoin de déclaration préalable jusqu'à 40 bits, libre avec déclaration préalable jusqu'à 128 bits (utilisation et importation).

U = utilisation, I = importation, E = exportation, F = fourniture

opération	pas de formalité	déclaration	autorisation
authentification	U	I, E, F	
clé $\leq$ 40 bits	U, I	F	E (?)
40 $<$ clé $\leq$ 128 bits	U, I (privé)	U, I, F	E

Projet de loi 3143 d'assouplissement de la législation, approuvé par le conseil des ministres du 13 juin 2001 (notamment article 37).

4.3. **En Europe.** Cf `http://ethesis.helsinki.fi/julkaisut/oik/julki/pg/parviainen/`.

Directive No 1334/2000 du 30 septembre 2000, remplace la directive de 1994 :
– l'exportation est complètement libre vers d'autres pays de la CE, sauf pour des produits très spécialisés comme ceux de cryptanalyse ;
– autorisation nécessaire pour exporter vers Australie, Canada, République Tchèque, Hongrie, Japon, Nouvelle Zélande, Norvège, Pologne, Suisse et USA, valide depuis n'importe quel pays de la CE ;
– pour autre pays, autorisation spécifique depuis chaque pays de la CE.