FONCTIONS DE HACHAGE CRYPTOGRAPHIQUES

SALUT! JE DOIS FAIRE UNE AFFICHE POUR LES DOCTORIALES QUI DÉCRIT MA THÈSE, MAIS J'AI UN PROBLÈME: J'AI RIEN FAIT PENDANT DEUX ANS ET JE SAURAIS PAS QUOI RACONTER. IL PARAIT QUE T'ES DOUÉE, TU POURRAIS M'AIDER? JE SUIS CENSÉ FAIRE DE LA "CRYPTO".

MOUI, SI TU VEUX

BON, LA CRYPTO C'EST UN DOMAINE PLUTÔT VASTE. TU ÉTUDIES QUOI EN THÉORIE?

J'AI OUBLIÉ...

OKAY.

BON, JE VAIS TE LISTER DES TRUCS CLASSIQUES ET TU M'ARRÊTES QUAND TU RETROUVES LA MÉMOIRE.

HMM, "PRIMITIVE" ÇA ME DIT QUELQUE CHOSE. ON A QU'À DIRE QUE JE FAIS ÇA.

LE BUT FONDAMENTAL DE LA CRYPTO C'EST DE COMMUNIQUER EN LA PRÉSENCE D'ADVERSAIRES. POUR ÇA ON DÉFINIT DES PRIMITIVES, QUI SONT À LA BASE DE LA CONSTRUCTION DE SYSTÈMES DE CHIFFREMENT.

C'EST UN BON DÉBUT MAIS ON AURA BESOIN D'ÊTRE PLUS PRÉCIS. IL Y A DES PRIMITIVES À CLEF PUBLIQUE (CHIFFREMENT RSA, ÉCHANGE DE CLEF DIFFIE-HELLMAN (SUR CORPS FINI, COURBE ELLIPTIQUE)...) ET À CLEF SECRÈTE (CHIFFRES PAR BLOC, FONCTIONS DE HACHAGE...

FONCTION DE HACHAGE! JE SUIS SÛR QUE C'EST ÇA. J'AVAIS RETENU LE NOM MAIS JE SAIS PLUS À QUOI ÇA RESSEMBLE.

DE FAÇON GÉNÉRALE, C'EST UNE APPLICATION DE $\{0,1\}^*$ DANS $\{0,1\}^N$: ON VEUT "HACHER" DES DONNÉES DE TAILLE QUELCONQUE VERS DES EMPREINTES DE TAILLE FIXE.

OÙ EST LA CLEF DANS TOUT ÇA?

DONC ON PEUT FAIRE N'IMPORTE QUOI?

EN FAIT IL N'Y EN A PAS (C'EST UN CAS UN PEU PARTICULIER).

SÛREMENT PAS!

Mi

UNE BONNE F.H. DOIT RÉSISTER AUX COLLISIONS : IL EST DUR DE TROUVER M, M' TELS QUE $H(M) = H(M')$. ON PEUT FAIRE ÇA GÉNÉRIQUEMENT EN $2^{N/2}$ POUR DES EMPREINTES DE N BITS GRÂCE AU PARADOXE DES ANNIVERSAIRES, MAIS ÇA DOIT PAS ÊTRE POSSIBLE DE FAIRE MIEUX.
DE MÊME LA F.H. DOIT RÉSISTER AUX PRÉIMAGES: SOIT C, ON NE PEUT PAS TROUVER M TEL QUE $H(M) = C$ EN MOINS DE 2^N.

A

DU COUP COMMENT ÇA SE CONSTRUIT UNE BONNE F.H.?

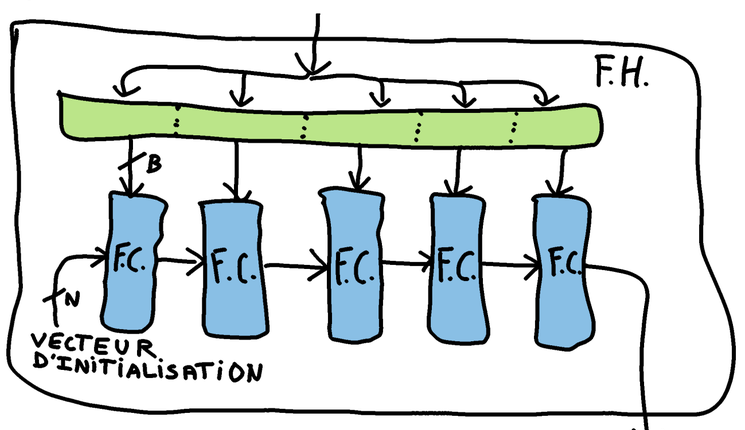
IL Y A PLUSIEURS FAÇONS, MAIS UNE DES PLUS SIMPLES, C'EST DE PARTIR D'UNE FONCTION DE COMPRESSION F.C. : $\{0,1\}^N \times \{0,1\}^B \to \{0,1\}^N$ ET D'UTILISER UN EXTENDEUR DE DOMAINE COMME MERKLE-DAMGÅRD.

ÇA PERMET DE RÉDUIRE LA SÉCURITÉ DE LA F.H. À CELLE DE LA F.C..

COOL.

CONSTRUCTION MERKLE-DAMGÅRD

UN LONG MESSAGE À HACHER QU'ON DÉCOUPE EN BLOCS DE TAILLE FIXE, COMPLÉTÉ SI NÉCESSAIRE ********



ATTAQUE SUR F.H. ⇒ ATT. SUR F.C.
¬ ATT. SUR F.C. ⇒ ¬ ATT. SUR F.H.

ET DONC, UNE FOIS QU'ON A UNE BONNE FONCTION TOUT EST FINI?

PAS VRAIMENT... EN FAIT ON ESSAYE TOUJOURS DE TROUVER DES ATTAQUES POUR MONTRER QU'UNE FONCTION Y RÉSISTE (OU NON).
JE T'EXPLIQUERAIS BIEN LES AVANCÉES RÉCENTES EN COLLISIONS SUR SHA-1, MAIS J'AI PEUR QU'ON MANQUE DE TEMPS.
QU'EST-CE QUE TU DIRAIS D'UNE PRÉSENTATION D'APPLICATION À LA PLACE?

OUI, BONNE IDÉE!

1

SI ON REPREND LES CHOSES DE PLUS HAUT, UN DES TRUCS UTILES QU'ON PEUT CONSTRUIRE EN CRYPTO, C'EST LES SIGNATURES ÉLECTRONIQUES: ÇA PERMET PAR EX. DE COMMUNIQUER AVEC UN SITE WEB DE CONFIANCE OU DE PAYER SES IMPÔTS EN LIGNE.

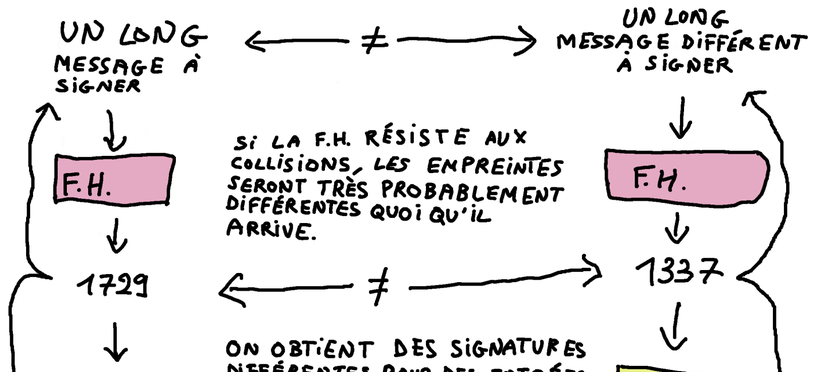
POUR FAIRE ÇA, ON SE BASE SUR DES PRIMITIVES À CLEF PUBLIQUE, MAIS ELLES ONT DES INCONVÉNIENTS: ELLES SONT LENTES ET NE MARCHENT PAS TOUJOURS BIEN AVEC DE LONGS MESSAGES.
UNE SOLUTION, C'EST DE D'ABORD HACHER LE MESSAGE ET DE NE SIGNER QUE L'EMPREINTE, QUI EST COURTE.

EUH, COOL.

MALIN.

2

HACHER & SIGNER



COOL MAIS, EUH Y A UN TRUC QUE J'AI PAS BIEN COMPRIS DEPUIS TOUT À L'HEURE: CETTE HISTOIRE D'ANNIVERSAIRES ET DE COLLISIONS EN $2^{\frac{N}{2}}$

C'EST UN PEU SURPRENANT.

AH, OUI. CE QUE ÇA DIT, C'EST QUE SI ON TIRE DES ÉLÉMENTS AU HASARD DANS UN ESPACE DE TAILLE N, ON VA TOMBER SUR UN ÉLÉMENT QU'ON A DÉJÀ VU AVEC BONNE PROBABILITÉ AU BOUT DE $\sqrt{N}$ ESSAIS.
LE NOM VIENT DU FAIT QU'À PARTIR D'UN GROUPE DE $\sqrt{365} \approx 20$ PERSONNES, ON A UNE BONNE CHANCE D'EN TROUVER DEUX AVEC LE MÊME ANNIVERSAIRE.

C'EST POUR ÇA QU'ON APPELLE ÇA UN "PARADOXE", MÊME SI C'EN EST PAS VRAIMENT UN...

8

ET, HMM "POURQUOI ÇA MARCHE"?

L'INTUITION C'EST QUE x ÉLÉMENTS DÉFINISSENT $\approx x^2$ PAIRES. CHAQUE PAIRE A PROBABILITÉ $\frac{1}{N}$ DE FORMER UNE COLLISION, DONC EN PRENANT $x = \sqrt{N}$ ON PEUT BIEN ESPÉRER EN TROUVER UNE.

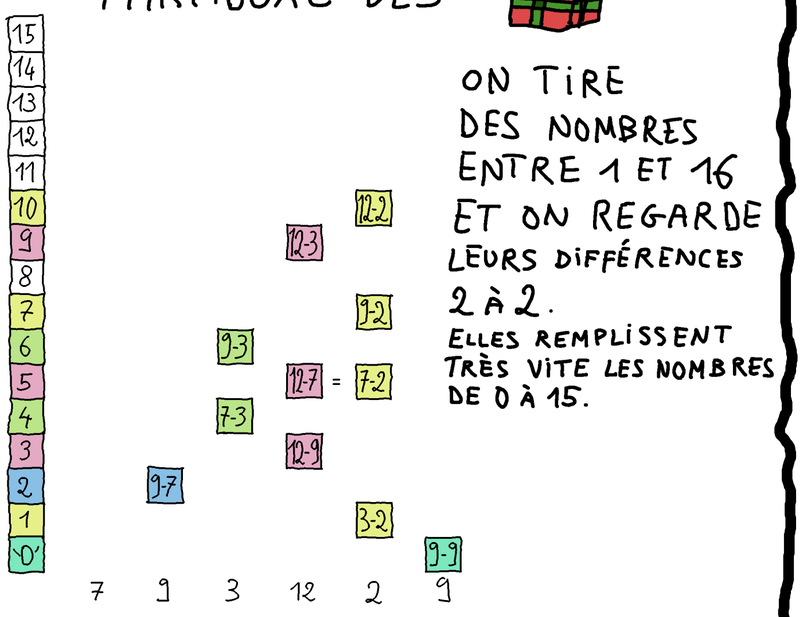
C'EST UN PRINCIPE ÉLÉMENTAIRE, MAIS ON LE RETROUVE SOUVENT EN CRYPTO DONC C'EST BIEN DE L'AVOIR À L'ESPRIT!

COOL! MERCI POUR TOUT.
DIS, TU VOUDRAIS PAS RÉDIGER MA THÈSE AU FINAL?

...

45

PARADOXE DES



ON TIRE DES NOMBRES ENTRE 1 ET 16 ET ON REGARDE LEURS DIFFÉRENCES 2 À 2.
ELLES REMPLISSENT TRÈS VITE LES NOMBRES DE 0 À 15.

Pierre KARPMAN

DOCTORANT
ÉCOLE POLYTECHNIQUE
+
NANYANG TECH. UNIVERSITY
pierre.karpman@inria.fr