Exo-Map.

Christophe Delaunay.

Crypto et pb du log discret.

Cryptologie = sc du secret.

— analyse = étude des messages secrets pour les décoder.

— gramme = message secret.

Ac : il faut deux coder / décoder.

- Confidentialité = texte non lu par un intrus
- Authentification = sûr de l'auteur
- Intégrité = message non modifié lors de la transmission
- non-répudiation : exp ne peut nier être l'auteur du message.

2 cryptographies : écrire à clef secrète] simple.

— publique : pour crypter.

pour décoder, il faut une clé secrète

Auj : "AES" : clef secrète : très rapide
(clé secrète :)

pb : - pour n personnes, il faut $\binom{n}{2}$ clés.

- pour communiquer les clés.

(clé publique) : il faut f f° telle que f soit facile à calculer
difficile à inverser

Rivest, Shamir, Adleman : RSA 1977

"multiplier deux entiers : facile
"factoriser : difficile".

El Gamal
DSA
Courbes elliptiques

$G = \{1, g, \dots, g^{n-1}\}$. On suppose que la $\times^{ion}$ se calcule rapidement.

$(g, \ell) \longmapsto g^\ell$ rapide.

Pour $y \in G$, trouver ℓ tq que $g^\ell = y$ est le pb du log discret.

$$\ell = \log_g y$$

Ce pb est difficile, mais on ne sait pas démontrer qu'il le soit.

Protocole Diffie-Hellman.

Alice et Bob : Groupe G, $g \in G$, d'ordre n.

A choisit k_A, calcule $y_A = g^{k_A}$

B —— k_B, calcule $y_B = g^{k_B}$

A reçoit y_B calcule $(y_B)^{k_A} = g^{k_B k_A}$

B —— y_A —— $(y_A)^{k_B} = g^{k_A k_B}$ = c'est leur secret commun.

Espion : Eve ou Charlie, connait G, g, g^{k_A}, g^{k_B}.
Il doit calculer $g^{k_A k_B}$.
Heuristique : c'est aussi difficile que le pb du log discret.
(mais on ne sait pas le démontrer)

(!) Pb de l'homme du milieu. Seule solution : Organisme de certification

$$g^\ell = \begin{cases} (g^{\frac{\ell}{2}})^2 & \text{si } \ell \text{ pair} \\ g(g^{\frac{\ell-1}{2}})^2 & \text{si } \ell \text{ impair} \end{cases}$$

Calcul nécessite $2 \log_2 \ell$

on peut encore baisser ~~[illegible]~~, mais en deça de $2\log_2 \ell$, c'est difficile

→ calcul linéaire en $\log \ell$.

Calcul en $O(\log \ell) = O(e^{\log\log \ell})$: c'est linéaire, i.e. très facile ⑨

$O(\log \ell^k) = O(e^{k \log\log \ell})$ polynomial. facile

$O(e^{(k+\log \ell)^a (\log\log \ell)^{1-a}})$ sous-exponentiel. compliqué

$O(\ell) = O(e^{\log \ell})$ très compliqué.

On a : - $g \mapsto g^\ell$ très facile.

- Décider si ℓ est premier polynomial
- Factoriser ℓ : sous-exponentiel

Réduction : $n = pq$ $pu + qv = 1$

$y^{pu} = (g^p)^{\ell_1}$ et c'est dans un groupe d'ordre q

$y^{qv} = (g^q)^{\ell_2}$ ——— p

$y = y^{pu+qv} = y^{p\ell_1 + q\ell_2}$

Si g est d'ordre p^m avec p premier, on ne peut pas faire cela.

C'est donc ce qu'on va faire.

Mais cela se réduit à un pb mod p, p^2, ..., p^m ...

Il faut donc choisir des groupes d'ordre q.

Algorithme Baby-Steps / Giant-Steps. (1960-1970)

Si $\#G = n$, soit $m = \lceil \sqrt{n} \rceil$ et $y = g^\ell = g^{km+r}$ avec $r < m$.

$y g^{-r} = (g^m)^k$.

gauche	droite
$(g^m)^0$	$y g^{-0}$
⋮	⋮
$(g^m)^{k-1}$	$y g^{-r}$

Il y aura une collision $(g^m)^k = y g^{-r}$ et donc $y = g^{km+r}$

→ on est passé de n à $\sqrt{n}$ étapes.

Pb : le stockage peut prendre bcp de place mémoire.

→ C'est basé sur le paradoxe des anniversaires :
choisir $\sqrt{n}$ elts dans n elts, il y a plus d'1 chance
de choisir 2 mêmes éléments. → méthode non déterministe.

Th de Shoup : Ds un groupe <u>générique</u> il faut $O(n^{1-\epsilon})$
i.e. en n'utilisant que la xion.

$G = (\mathbb{Z}/n\mathbb{Z}, +)$, $g = 1$: $y = \ell \cdot 1$: c'est trivial.

$G = (\mathbb{Z}/p\mathbb{Z})^{\times}$, g générateur ; on voudrait que p − 1 soit presque premier.

PARI (Henri Cohen, de la thèse de Christophe Delaunay)
↳ le plus populaire.

$(\mathbb{Z}/p\mathbb{Z})^{\times}$ $\frac{p-1}{2}$ premier.

Conjecture : on le trouve facilement.
→ on ne sait pas s'il y en a une infinité.

Le pb du log discret se résout en $O(e^{c(\log p)^{1/3}(\log\log p)^{2/3}})$ xions

Autres groupes : gps de pts d'une courbe elliptique.

Puis on cherche un générateur du groupe : l'h gp de Riemann assure qu'on le trouve rapidement.

courbe elliptique : $y^2 = x^3 + ax + b$ $a, b \in \mathbb{Q}$.

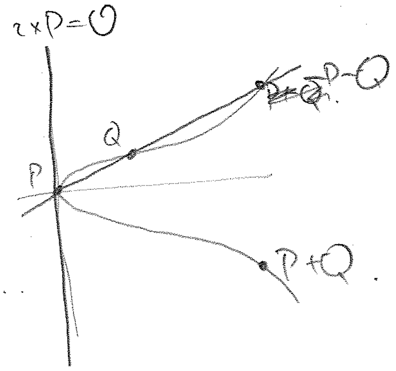
lisse si $4a^3 + 27b^2 \neq 0$.

pts de $E = \{(x,y) \in \mathbb{Q}^2 : y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\}$
pt à l'infini.

$E(k)$: loi naturelle :

$P, Q \in E(k)$: la droite passant par P et Q repasse par un 3ᵉ point. on en prendra le symétrique.

$\mathcal{O}$ est le neutre.



$k = \mathbb{F}_7$. $E : y^2 = x^3 + x + 4$.

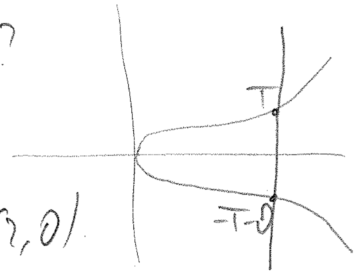
$E(\mathbb{F}_7) = \langle (0,2) \rangle = \{\mathcal{O}, (0,2), 2\cdot(0,2), \dots$

$(2,0) \in E$.

$= l \cdot (0,2)$. Mais que vaut l ?

or $2 \cdot (2,0) = l$.

Ici on trouve $5 \cdot (0,2) = (2,0)$



Si E défini sur $\mathbb{F}_p$ avec p grand : difficile.

Trouver E et G tels que $\#E(\mathbb{F}_p)$ presque premier.

Trouver un G à

$\#E(\mathbb{F}_p) = p + 1 - t$ erreur de l'heuristique
heuristique

Th : $|t| \leq 2\sqrt{p}$. et t se calcule en temps polynomial.

Application :

E sur $\mathbb{F}_5$

E et $\#E(\mathbb{F}_p)$. On veut de la forme cq. Sinon on recommence

$p = 2^{192} - 2^{32} - 2^{12} - 2^8 - 2^7 - 2^6 - 2^3 - 1$

il s'écrit très simplement en base 2.

Courbe : $y^2 = x^3 + 3$.

et on a la courbe "secp192k1"

Si $t = 1$ Attaque de Smart (linéaire !) (courbe de Tate).

Si $t = 0$ —— sous-exponentielle.

Courbe elliptique : permettent de factoriser.

certifier la primalité

Factoriser avec les C.E. : Si N n'est pas premier, on fait plein de calculs jusqu'à ce que ça bloque.