
Sem. 1-3 Sept 2010

CRYPTOGRAPHIE

- ✓ Réalisation d'une interface pédagogique sur le codage/décodage de messages avec clés RSA
  - Sous Processing
  - Utilisation de la librairie ControlP5 pour le rendu de l'interface
  - Scénario: on imagine qu'il puisse se faire par l'intermédiaire d'un serveur web local, afin de permettre les actions séparées de deux protagonistes, Alice et Bob.

1. Alice est chargée de générer les clés publique et privée en suivant les différentes étapes: 1) génération de deux entiers premiers P et Q; 2) Calcul de N=PxQ; 3) Générer E tel que E soit premier avec (P-1)*(Q-1); 4) Calculer D selon: Il existe un relatif entier M, tel que $E \times D + M \times (P - 1)(Q - 1) = 1$
-> (N,E) est la clé publique; D est la clé privée
Alice divulgue la clé publique et garde précieusement la clé privée.

2. Bob reçoit la clé publique. Il écrit son message secret, il le traduit en chiffres. Il encrypte ensuite le résultat grâce à la clé publique. Il envoit le message encrypté à Alice.

3. Alice reçoit le message encrypté. Elle le décrypte grâce à sa clé privée. Elle obtient une suite de chiffres qu'elle traduit en lettres et aboutit au message secret de Bob.

- x A FAIRE: action supplémentaire: demande d'authentification de Bob vers Alice.
- x A FAIRE: Nettoyer le code de telle sorte que les fonctions relatives à l'interface et au calcul/manipulation des clés soient séparées.

LE SON

- ✓ Réalisation d'une interface pédagogique sur les notions de contenu sonore et perception
  - Sous Processing
  - Utilisation des librairies: ControlP5 pour le rendu de l'interface,
    Minim pour l'input et output audio.
  - Un analyseur permet de visualiser le contenu fréquentiel du son en **temps réel** (par transformation de Fourier FFT) : quand je parle, et/ou fait tout bruit quelconque, les sons que je produit sont analyser en temps réel
  - Une interface de manipulation permet d'émettre une sinusoïde ou de charger un extrait sonore de son choix, musical ou davantage assimilable à du bruit.
  - Par la fenêtre de l'analyseur, on visualise les signaux **en temporel et en fréquentiel**.
  - La position de la souris sur la fenêtre de l'analyseur permet d'ajuster le volume de la sinusoide et de l'extrait sonore (haut/bas), et la fréquence de la sinusoide (gauche/droite)
  - Un filtre passe-bas peut être appliqué sur l'extrait sonore. Son résultat peut être perçu auditivement mais aussi est visualisé en temporel et en fréquentiel.

- x A FAIRE: Nettoyer le code de telle sorte que les fonctions relatives à l'interface et au calcul/manipulation des signaux soient séparés

---

Entrevue avec Philippe, auteur de Javascool V3:

- ✓ Accord pour la mise en place de **deux phases** dans le processus pédagogique:

1. Manipulation d'une interface réalisée sous Processing qui aborde un sujet à 'consonance' informatique, par example la cryptographie, ou acoustique, etc. Une interface avec plusieurs boutons d'intéractions, cette première phase est celle de l'exploration du sujet.
   - x A FAIRE: L'interface sera proposée sous forme d'API
2. On profite du contexte, de l'exploration d'un sujet pour coder: accès aux commandes clés du programme de l'interface manipulée lors de la phase 1, ajustement/modification de certaines commandes.
   - x A FAIRE: La phase 1 met donc en place la liste des commandes qui seront accessibles lors de la phase 2 ('play sinusoid', 'encode message', etc..).

Entrevue avec Julien Holtzler, membre actif de POBOT, association de robotique sur Sophia:

✓ Idées:
- une réalisation de Pobot en prêt pour l'espace muséal de l'Inria.
- une rencontre prochaine pour découvrir une partie de leurs réalisations
- une intervention/collaboration pour intervenir en milieu scolaire?

Sem. 6-10 Sept 2010

LE SON

✓ Réalisation d'une interface pédagogique sur la synthèse sonore, ou comment à partir de sons isolés numériques, synthétiques ou 'naturels', compose une phrasé pseudo-musical, mais surtout qui prend une dimension autre que les sons pris isolément. Il s'agit d'un sonar qui balaye des sources provoquant leur déclenchement.

- Sous Processing
- Utilisation de la librairie Minim pour l'input et output audio.
- Sons: enregistrement en temps réel, chargement d'extrait sonore. x
  A FAIRE: pouvoir déclencher une sinusoïde ajustable en fréquence et amortissement.
- Les sources sonores sont symbolisées par des balises carrés. Les balises peuvent déplacées sur le sonar, impliquant un enchainement/rhythme différent. La position de la balise par rapport au centre du centre détermine l'amplitude sonore donnée à la source: plus la balise est proche du centre, plus son amplitude sera importante.
- La vitesse de balayage est ajustable en temps réel, par < >, on peut aussi aboutir a des valeurs négatives et donc le sonar change de sens de balayage. La vitesse est inscrite comme indication sur l'interface.
- Chaque source peut être sélectionnée tour à tour; pour accéder à une en particulier, on utilise: ^ v . Elle apparait alors avec un contour blanc plus prononcé. La source sélectionnée peut être déplacée, ou encore supprimée. Le volume sonore de la source sélectionnée est inscrite sur l'interface.
- Le sonar peut être arrêté, stoppant l'émission de l'enchainement sonore.
- x A FAIRE: des effets sur les sources sonores (pan, filtre)?? des liens entre les sources enchainées?? (le balayage du sonar détermine l'enchainement non?)
- x A FAIRE: problème à résoudre: spasme lors du déclenchement de la source sonore; solution: déclencher en fonction de la congruence avec frameCount et non pas en fonction de la position du balayage!

LES GRAPHES

- Idées:
  - Une voiture sur un terrain en 3D qui doit sortir d'un labyrinthe (algo de Pledge)
  - La voiture génère des petits doit parcourir une distance d'un point de départ à un point d'arrivée (algo du plus court chemin).
  - Une source: la thèse de Léa Cartier, en cours de lecture.
  - x A FAIRE: tout

- Rencontre en perspective avec Philippe Luc le 21/09 pour discuter du programme des TES autour de ce sujet.

INFO / ROBOTIQUE

- Rencontre en perspective avec Laurent Brunetto autour de l'info/robotique, ce qu'il a en tête:
  - Présentation de l'ordinateur et des grandes fonctions/périphériques
  - Histoire de l'info et découvertes
  - Recherches des élèves pour exposés sur ces thématiques
  - Initiation à la programmation Java/Basic
  - Application à la programmation des micro-controleurs PicAxe :
  - http://www.rev-ed.co.uk/docs/AXE020.pdf

- Initiation à quelques capteurs simple
- Réalisation de modules simplifiés
- Réalisation d'un mini robot détecteur d'obstacle/suiveur de ligne.

Sem. 13-17 Sept 2010

- INTEGRATION applet processing dans javascool

1. Le fichier .pde principal de la papplet processing est exporté afin de générer les différents fichiers java nécessaires à l'intégration
2. Grâce au makefile construit par Thierry, les différentes routines sont appelées automatiquement lors du chargement de javascool pour permettre l'intégration, visualisation et intéraction, des applis initialement générées en processing.
3. Pour permettre une intégration adéquate, on doit rajouter dans le fichier principal .pde:
   - frame = nex Frame()
   - getInterface()

- Nouvelle arborescence dans GForge: Sketchbook au-dessus de proglets
  - ExplorationSonore et CryptageRSA
- Commit: copier fichiers nvx puis "make svn" au plus haut niveau pr commiter

- Le problème d'usage de controlP5? Pour tester, construction de deux fenêtres indépendantes sans controlP5, à tester dans javascool pour voir si l'intégration est plus adéquate.

LE SON

- Interface pédagogique sur les notions de contenu sonore et perception:
  - résolution des problèmes de tailles de fenêtre pour l'intégration dans javascool
  - dissociation des parties de code concernant l'interface (boutons, apparence, etc...) et les fonctions (émet une sinusoide, lance un enregistrement, etc...)
  - création de deux classes: enregistrement et sinusoide (est-ce nécessaire?)
  - résolution des messages de warning
  - résolution du problème d'analyse et traçage du signal de sortie: on peut à présent imaginer un setup avec écoute au casque!!
  - x A FAIRE: à continuer, en fonction des problèmes rencontrés,

- Interface pédagogique sur la synthèse sonore:
  - x A FAIRE: déclencher les sons en fonction de la congruence avec frameCount et non pas en fonction de la position du balayage!
  - difficile avec la configuration actuelle de radar sonore, essai avec une autre configuraion davantage linéaire, compo sonore, à étendre.

CRYPTOGRAPHIE

- Interface pédagogique sur le codage/décodage de messages avec clés RSA:
  - dissociation des parties de code concernant l'interface (boutons, apparence, etc...) et les fonctions (émet une sinusoide, lance un enregistrement, etc...)
  - résolution des messages de warning

LES GRAPHES

- Concepts premiers sur la théorie des graphes, sensibiliser à l'algo du plus court chemin
  - site de référence: http://www.imathematics.fr/ !! (David Marec contacté), aucune réponse à ce jr

  - ID:
    - créer graphe 2D
    - à chaque noeud, la voiture se clone et chaque clone garde en lui le chemin deja parcouru;
    - la première arrivée lance un signal, la première à parcourir tous les noeuds lance un signal.

    - Pré-illustration avec une petite voiture se baladant dans un environnement 3D, qui devrait optimiser son chemin, ; des etapes à atteindre représentront les noeuds du graphe 2D

  - x A FAIRE: TOUT

_____
_____

Sem. 20-24 Sept 2010
_____

LES GRAPHES

- Concepts premiers sur la théorie des graphes, sensibiliser à l'algo du plus court chemin
  - mise à disposition du code de D. Marec, site de référence: http://www.imathematics.fr/ !! ; volonté de sa part de partager et collaborer

  - construction avec Thierry d'un squelette de classe Graph, avec fonctions principales
  - élaboration du code à partir de ce squelette pour la construction d'une appli capable de:
    - créer une population de noeuds,
    - créer des liens entre les noeuds,
    - effacer un noeud et/ou un lien,
    - afficher les infos de distances pondérées (poids=valeur de la distance)
    - bouger les noeuds dans la représentation
    - calculer un chemin optimum entre deux noeuds.

  - x A FAIRE: continuer avec intégration de l'algo de Dijkstra, enrichir avec le code de D. Marec.

_____

LE SON

- Interface pédagogique sur la synthèse sonore:
  - les sons se déclenchent en fonction de la congruence avec frameCount et non pas en fonction de la position du balayage!
  - x A FAIRE: améliorer la lisibilité de l'interface, intégrer toutes les fonctionnalités discutées avec Thierry, en faire une API avec les fonctions tel que addSource, displaySource etc..

_____

Le but à présent est de faire des papplets des API afin que certaines fonctions principales soient accessibles/ manipulables par les élèves.

_____
_____

Sem. 27 Sept - 1er Oct 2010
_____

LE SON

- Interface pédagogique sur les notions de contenu sonore et perception:
  - possibilités de générer plusieurs types de signaux en plus de la sinusoide, un signal carré, un signal scie et du bruit (blanc),
  - création de trois fonctions addSignal(n,f,a), addRecord(n) et stopAnySound() en vue de la manipulation par les élèves

- factorisation du code: suppression de la redondance de drawFFT et drawSignal en prenant un argument en entrée correspondant à out, player ou in.
- création de la doc Doc.rtf explicative, introductive au travail
- création de son about-proglet.xml

- Merging de l'interface dans la fenêtre de visualisation: amélioration pr le portage dans javascool (on espère), et pour visualisation sur le web

---

LES GRAPHES

- Concepts premiers sur la théorie des graphes, sensibiliser à l'algo du plus court chemin
  - création de la doc Doc.rtf explicative, introductive au travail
  - création de son about-proglet.xml
  - bug résolu lorsque display du plus court chemin entre 2 noeuds..
  - des instructions qui se déroulent sans controlP5!, du coup l'interface est dégagé pour les graphes
  - x A FAIRE: la voiture dans un environnement 3D (l'idée étant de proposer différents niveaux d'approches, dc différentes applets)

CRYPTOGRAPHIE

- Interface pédagogique sur le codage/décodage de messages avec clés RSA:
  - création de trois fonctions createKeys(), encrypt(String mess, BigInteger publicKey) et decrypt(BigInteger mess, BigInteger Keys) en vue de la manipulation par les élèves
  - les différentes étapes de la création des clés est expliqué (du type N = P*Q)

  - x A FAIRE: merger les 2 fenêtres en une avec des zones qui s'activent selon qui manipule, cad Alice ou Bob.

Rencontre avec Joanna J. d'Interstices:

- envoi de videos illustrant les proglets, en vue d'une possible intégration dans Interstices? Peut être pour celle "exploration sonore", avec possible texte d'explication

- possible contribution pour un article relatif à la thèse

Discussion avec Philippe Luc pour une intervention possible sur le son, avec comme appui l'applet
- intervention en plusieurs temps: explication son/acoustique, manipulation applet, programmation, voire explication codage mp3

Sem. 3 - 8 Oct 2010

CRYPTOGRAPHIE

- Interface pédagogique sur le codage/décodage de messages avec clés RSA:
  - les 2 fenêtres Alice et Bob sont rassemblées en une avec des zones qui s'activent selon qui manipule. Permet une meilleure intégration de la fenêtre dans javascool, et/ou une meilleure gestion du popup

---

LES GRAPHES

- Concepts premiers sur la théorie des graphes, sensibiliser à l'algo du plus court chemin
  - la voiture dans un environnement 3D
  - appli introductive aux concepts liés aux graphes: une petite voiture se balade entre différentes stations et valide des chemins entre ces différentes destinations, le but étant d'effectuer manuellement le plus court chemin d'un point à un autre
  - on propose de trouver le plus court chemin entre 2 villes, en visitant 2 villes supplémentaires; l'élève l'effectue à tatons et s'il le trouve, on lui dit BRAVO!
  - activité possible pour la proglet: getVisitedSpots (renvoie les villes vistées par la voiture)

Réorganisation des fichiers:
- ExplorationSonore est l'interface unique, tandis que sa version à deux fenêtres se nomme ExplorationSonoreV1
- UnGrapheDesChemins pour GrapheAPI, EnVoiture pour la version 3D

Discussion avec Philippe Luc pour une intervention possible sur le son, avec comme appui l'applet
- Séance 1 autour de la psychoacoustique (voir notes), faire re-découvrir le son, extraire des impressions
- Séance 2 sur le signal, et l'introduction à l'applet: brève manipulation collective, puis individuelle; pour ensuite laisser programmer via la proglet