

Cours Sécurité : Travaux pratiques 2011–2012

19 octobre 2011

Modalités de contrôle Les travaux pratiques sont effectués et soutenus en *binôme*. Les TP 1, 3, 5 et 7 seront évalués. Il s'agit de rendre un rapport succinct expliquant votre démarche et vos solutions et de faire une soutenance (10min de présentation + 10min de questions). Les TP 1 et 3 sont évalués ensemble. Voici les dates de soutenances :

- TP1 et TP3 : 22 novembre,
- TP5 : 29 novembre,
- TP7 : 6 décembre.

Chaque rapport est à rendre par mail le jeudi précédant la soutenance. Les retardataires seront pénalisés. À titre indicatif, l'évaluation du TP5 aura un poids supérieur aux TP1+TP3 et TP7, alors que ces derniers auront un poids comparable. Juste après la soutenance un membre du binôme doit envoyer un message avec les sources à

sylvain.perifel@lifa.jussieu.fr

avec comme sujet [SECURITE]. Le message contiendra en attaché un repertoire avec le code source comprimé selon le standard tar.gz. Le code doit être commenté et le repertoire doit contenir un fichier README qui explique comment utiliser les sources.

Sur le plagiat Des textes sur ce qu'on considère comme un plagiat dans un environnement académique sont disponibles aux pages

<http://www.pps.jussieu.fr/~amadio/Ens/editions-plagiats.pdf> et

<http://wiki.univ-paris5.fr/wiki/Plagiats>.

Le plagiat est une forme de fraude et il est sanctionné selon le règlement de l'Université Paris Diderot (voir <http://www.pps.jussieu.fr/~amadio/Ens/plagiats.pdf>). En particulier, dans ce cours il n'est pas admissible (1) de présenter un code qu'on ne comprend pas et (2) de présenter un code trouvé sur internet et/ou copié d'un autre projet sans le mentionner *explicitement*. A noter que dans le deuxième cas, la *sanction minimale* proposée au jury est que *tous* les membres des projets qui partagent le même code aient comme note de projet 0/20.

TP1 : Utilisation de Gnu Privacy Guard

GnuPG est un logiciel *libre* qui met en œuvre différents aspects de la cryptographie à clé publique traités dans le cours (chiffrement ElGamal, signature DSA, ...).

L'objectif de ce travail pratique est d'apprendre à utiliser le logiciel GnuPG et de préparer une démonstration de 5min de ce qu'on a appris.

Le logiciel est disponible à l'adresse <http://www.gnupg.org/> et il est décrit dans le manuel GnuPG disponible à la page

<http://www.gnupg.org/documentation/>.

Voici certains points que vous pouvez aborder dans votre démonstration :

1. Une démonstration des fonctionnalités de base du logiciel (vous pouvez vous inspirer du premier chapitre du manuel).
2. GNUPG offre des nombreuses possibilités d'interface avec d'autres logiciels (par exemples avec des programmes pour la gestion du courrier électronique). Voir

http://www.gnupg.org/related_software/

Vous êtes invités à préparer une démonstration de certaines de ces possibilités.

3. GNUPG adopte un modèle pour la gestion des clés qui est basé sur une toile de confiance (voir chapitre 3 du manuel). Vous êtes invités à expliquer par des exemples ce mécanisme.

Le rapport fera une page au maximum.

TP2 : Cryptoanalyse de chiffrements affines (introduction)

Le but de ce TP est de se familiariser avec les programmes disponibles sur le site

<http://www.apprendre-en-ligne.net/crypto/menu/index.html>

afin d'analyser des textes chiffrés avec des systèmes affines.

NB Pour manipuler les textes chiffrés, il convient d'utiliser un lecteur de pdf permettant le copier-coller.

Vigenère

Considérez le texte chiffré suivant dont on sait que le texte clair est en anglais et que la méthode de chiffrement utilisée est celle de Vigenère.

LPEKW YAJPP RTRJQ FITFU PEGIN GLKRV RZQDM PBAPG SMSPC WEALG
RFBES PFWVC CNUCQ SLZEV YPOKV TYRXK LGQNT SZCEA EKWUH VVLOA
IAXWF IEHZE SIXWG MHVFD TDXAZ OCSIS LOTRC JMVIK VLOY S LQUVU
ISDZC GKVNG RJOET ZROQF KTRBO HSEPO KVHVI DPZJW JGQKK VZFRL
PIDKC VKTES SOBHK CKICP DSNKG PVVFD LEMKV KQSYS HLDGK VKKDV
FTYRM JPWTO NBXTY HWAOG LCODD SIYWM NDWCC ESI DW LFAPA LOPLA
ZXGEC JPCJW HMWRY RBODE YLQVY HVHSP CXDMH NERGF CPSBU SMI EU
LOLMO GUJAZ BHZFP ZJWYO IHSES IPZGW BCSZO RIPBA PGLDL YOTEK
CKNXH SPOEE AAGSN VPYDY ZLWPL POHST XAZSD BZHHT ELLQF MEPSD
CLRYT GUESM SPC

Le site propose différentes méthodes pour retrouver le texte clair et la clé. Par exemple :

1. méthode de Babbage/Kasiski,
2. méthode de Bazeris,
3. méthode basée sur l'indice de coïncidence.

Appliquer ces méthodes au texte en question.

Permutation

Décryptez le texte suivant obtenu par application d'un chiffrement par permutation (on dit aussi transposition) d'un texte français.

EURNU USPOR EIUCF ENPRS RNETV AATUE ULCRE BMRSA EAETL TLETI
 ONATN ENMET OCEUD QNTE IUOAS RTCOV UAOQN NEUDI RNUSF UEUSO
 AMRDO SBSAE IYEOE RRDAC OUDTT SUTPI UEDQN EAEMM MUEUS FENOS
 DLANV IENPE HLECS SONTE AORGE TLSTU NNAOT UEIEQ SOIEM STITN
 RBONG EISAI ORNVA NYLEE IAEOD RTTCD UNIOF NSVAT ORQVS ZUGUE
 TLTEI EAUDEL LBRTU UEDEO BLLAO ESUIL RETDI TOUMN REEOC YKENW
 IUEVL ELSTN OBNTU UNDEO EAVDA TJAVI EOIDV SSUNU EEUIS BNLLS
 BTLSL EERED RETOE CEESN TSTRE OSDEP ESMX AUDEF IEHAC MSEM
 NNTSS UEEZO LPSEE SLCEA UNEOH CCSOT ILEV L SLESE DULRE ODSAB
 SELUR OUAMR VFEUS EEESL LENA O SLLLS RNPUE SLGET ESEEL GLAYA
 DTTNN EESAT GVRAU YELEO QNCSE IUTAD LLEAM LAELE ECLNL IERIA
 AEIPA EMENS NALOL NETPS AEBNT IEEST DNAIL AEIER SSTIN AAPAB
 TUIUA OREDT RAEIP AEDEF AONNO EDURN EIMLO OCCRG ODICN SRMEE
 AOICA SFCHN FRCER LOTDO NEIUV TEEMN IENTE AELLB RIAUA EARAD

Y-a-t-il une relation entre l'indice de coïncidence du texte clair et du texte chiffré ?

Produit de Permutation et Vigenère

Le texte ci-dessous a été obtenu par un système cryptographique qui est le produit d'un système par permutation avec un système de Vigenère. Pouvez-vous retrouver le texte d'origine dont on sait qu'il est en français ?

XNBVT PTAIW IXWLC TAVZA RWTWT WGKVV VGUEY VZTAM MECIX FMZGA
 DBRGY WTYN PLMAR RCRWA TTJTQ GITWK LTJKQ UTPPE QGLPZ IRPUA
 YLPJT FKHVW HEXML XTANV WTEFV WIFUR QRRYX WMGVU RPNBW TITXM
 WIEMB IVVFP VORPG CMBAG EJIUV ETNKO KTVMC OMEVT ITNVA RCWTV
 XCKSK AVQVH YNAET KMHGT GRBIT DKZSP MXJWK VAVMV RXXSM IBJDC
 BTICU LCXSK WRPMJ ZXLHX KMBLV BWTIT XMMCK HCINM XPRTR DMEVH
 CHGZP HTXDW NRXAG UEGSX VBAXT IMFON DYLVW XFKAT HTVFA EJZTR
 CIQWE IBTCU ROPHP BCWIK WRTIT IKBMW SMVCE TIBBC CJOQG FHPLW
 BJLTD PYTVG CTURZ TUYJI XVTPU ZVWYA QTMBJ CLRPS TETKO AIWFQ
 EJMZU LBZMN BRGWK QIJCA NGYTY OZCSV CBTEF YXVNS ELQTP TIHBI
 IVQRO ZXEQW BGMTR GPAIX TXXUA GCMDW ECOXZ AYVEE MWAGH VCRQR
 XQHUN CKWQJ MTRXM LXDVF OSJSG QCJFI AVXXE XCLTJ ZFOYH TXKWX
 JWZKI BMCDL PRZRG EUTX XGGXH NJSST QKYSI RTMCS YMXIV AZVNN
 YTFXC ZOEGF SITMK VZMWX EIINV MELVV DLDXM WFDVU NWEXJ MZMMR
 BRPSS EBZNX VQDTR BGLWX PZMVT HKXKM TVRUA CXT