Cryptography, winter 2015/16

MICHAEL NÜSKEN, SIMON SCHNEIDER

2. Exercise sheet
Hand in solutions until Friday, 13 November 2015, 23:59

Exercise 2.1 (Break Vigenère). (8+4 points)

The following text is a Vigènere encryption.

> ZLL PIEZ UBIAFOSU AIE GWRIL RUV ALM ROVZX BUSI, OETR OR QIAF, UR TEG 21, 2061, MZ E AMUQ CLLR PGSEUMBK LMYWB EZIWTMP ORAS BTK PPKPF. ZLL UCQYXPSV OGQL EJAAX HW I DKWBPB AL E MMDQ-JSSPID HIA SDQX LPKPNGPSW, IZJ MA LIBVIUIL FNMZ AIK:
>
> GPLBIZJIY ELQRP HRL NKVAVIY RYWSD IKVL XEA UJ ALM RGMALNGR EAXMZJEUXA AL QBPBUBEJ. EA IKPS EA MTC OYUMT FLMVSY GVYTP, ZLLC SZKA DLIF REF FMTORK XPQ ISSH, KXOGRMVS, LPHWPUTK MEKQ – SMSIA MTH TMTQY SM JIOK – SM XPMZ KPEVF ISTTCFKV. ALMK NEK EB XKEZX I HGKBI VAZMVR WR ZLL KMZKVHP XXGR VJ ZQREFW IZJ GPVKGOXZ XPMZ LHH TATK ZMVOK KYSEZ VEZX BTK TVMVF CLLVM MTC ZMVSRI OYUMT GVYTP VSZWQNRC OEDQ G JPVU SXEZT WR ZLL APARI.
>
> TYTFOZHG EMY WLPN-MJNBWBUTK HRL EKPM-GWDXIJXQZM. MA LIP ZS II, NAX RVXPUTK OYUMT GVYTP GHQYAF GRK GWDXIJX QF WYPGSXE IUSCSN SY IDQT EKIYGGXLPG QTSBKP. EU EKITX GRK PCBUZ HXBQTHLH BTK QVRAFXSBW OUGRA SVXE PPKPFRC HRL EATLVNUIMHPTK, EIA EA IKPS EA MTC TIV OUYSH. BTKC MIL UZ HHXI, MJNBWBQJ UBIAFOSUW BA OXZ RMQJW HRL FXEUWTMZIK XPQ GRZAMDY XOEB IKVL MAEAIK. GMDZEPRTK ZLLC, IZJ ESP WFNIYW TUQI ALMY, CIYI NGRPF IVFOXSIL FU WOEZQ OR ALM SRSYC BTGX DEA YAPAMDMI’W.
>
> MSZ PKGHHME, SYSXQHGG OEL TKPWIL PKWPKV FNI ZLQBY EUH XXUX ALM FXEQIKFUVPIA FNEA IVMHPLH UMT XV VMMIL ALM YUSU, QIDY, EUH DQTYZ, FCF VEZX BTGX, LEZFN’W WSWD XIZSCDIIZ GWGRH USB EATWSZF ZLL WPUVW. ASW YAGO IVQXKF AIE TILHMP LSY XPQ RSUK BDOTZ. IIDZL LBXXUMAIL UZW JSIX GRK YZMTMBQ EUZL PRKDKEZMVS KJMMKUKRJC, JGZ XOIZQ CEZ SVXE WV QCON SM FWFN.
>
> FBX AXUASC UGRXPZIO RIHVVQJ IUSCSN XV EVECIY HMQVIY UCQYXPSVE SSYI NGTHHQMZZESPG, MTH VR UME 14, 2061, AOEB TGH IIMZ ZLLSZK, HIJEUQ LEJX.

(i) For $\tau = 1, 2, \ldots, 10$ compute $S_\tau = \sum_{i=0}^{25} q_{\tau,i}^2$ where $q_{\tau,i}$ is the frequency of the letter i in the ciphertext letters $c_1, c_{1+\tau}, c_{1+2\tau}, \ldots$. Let τ_0 be the value for which S_τ is closest to the 'English' value $\sum_{i=0}^{25} p_i^2 \approx 0.065$ where p_i is the frequency of letter i in English. $\boxed{4}$

+4 (ii) For each offset $a \in \{0, 1, 2, \ldots, \tau_0 - 1\}$ compute the key letter $k_a \in \{0, 1, 2, \ldots, 25\}$ for which $\sum_{i=0}^{25} p_i r_{a,i+k_a}$ is closest to 0.065. Here $r_{a,i}$ is the frequency of letter i in $c_a, c_{a+\tau}, c_{a+2\tau}, \ldots$.

4 (iii) Find the key k and decrypt.

Exercise 2.2. (6 points)

6 When using the one-time pad (Vernam's cipher) with the key $k = 0^\kappa$, it follows that $\text{Enc}_k(m) = m$ and the message is effectively sent in the clear. It has therefore been suggested to improve the one-time pad by only encrypting with a key $k \neq 0^\kappa$, ie. to have KeyGen choose k uniformly at random from the set of *non-zero* keys of length κ. Is this an improvement? In particular, is it still perfectly secret? Prove your answer.

If your answer is positive, explain why the one-time pad is not described in this way. If your answer is negative, reconcile this with the fact that encrypting with 0^κ doesn't change the plaintext.

Cosec computer security