Klasické šifry

Špecifikácia zadania

Tajný agent s krycím menom *X24* získal *2* zašifrované správy, jednu kratšiu a jednu dlhšiu. Pri tajnom odposluchu komunikujúcich sa zároveň dozvedel, že pre dešifrovanie hlavnej (dlhšej) správy potrebuje najprv dešifrovať tú kratšiu, ktorá obsahuje časť kľúča tej hlavnej správy. Žial, druhá časť kľúča k hlavnej správe nebola zistená. Náš agent však zistil použité spôsoby šifrovania:

- krátka správa bola šifrovaná Vigenerovou šifrou (s periodicky sa opakujúcim heslom), kde použitá dĺžka hesla bola *4* znaky;
- dlhá správa bola zašifrovaná jednoduchou substitúciou a následne prešifrovaná stĺpcovou transpozíciou s heslom dĺžky *20*.

Z odposluchu vieme, že posledných *20* znakov kratšieho textu obsahuje (po dešifrovaní) kľúč k transpozičnej časti (permutáciu použitú pri šifrovaní v tvare *a=0, b=1, ...*). Po získaní tohto hesla by bolo možné dešifrovať tú dlhšiu správu pomocou transpozície a úlohou by ostalo už len riešenie jednoduchej substitúcie. Zachytené správy boli písane v anglickom jazyku.

Agent *X24* potrebuje Vašu pomoc pri rozlúštení zachytených správ, ktoré musí do Vianoc doručiť svojmu veliteľovi.

V zadaní boli použité nasledovné klasické šifry:

- Vigenerova šifra s periodicky sa opakujúcim heslom;
- Šifra zložená z jednoduchej substitúcie a zo stĺpcovej transpozície.

Vstupy, výstupy:

K zadaniu máte priložené 2 šifrované texty:

- jednu kratšiu a
- jednu dlhšiu.

Pri hodnotení sa použijú podobné texty, avšak iné parametre.

Realizácia:

Naprogramujte konzolovú aplikáciu v programovacom jazyku Java, využite pri tom šablónu. Vstupom aplikácie sú 2 zašifrované texty s názvom "msg_short.txt" a "msg_long.txt", ktoré sú umiestnené v koreňovom priečinku (kde sa aplikácia spustí) a načítajú sa automaticky po spustení programu. Vašou úlohou je doprogramovať jednotlivé časti lúštenia do šablóny - do triedy *Solver*, kde sú predpripravené funkcie. V prípade, že potrebujete ďalšie funkcie a triedy, všetko dávajte do balíku *...zadanie2.student*. Triedu *Main* nemodifikujte. V zdrojovom kóde nikde nezadávajte absolútnu cestu, alebo inú, ako to je určené v zadaní.

Odovzdávanie:

Do AIS, miesto odovzdania. Deadline je 24.12.2021 do 12:00.

Odovzdávajú sa 2 priečinky (skomprimované do 1 ZIP súboru):

- priečinok "src" - zdrojové súbory s príponou .java (priečinok src) + všetky potrebné vstupy,
- priečinok "dokument" - jeden PDF súbor - správu (max 1-2 strany), kde máte zdokumentované ako ste postupovali a aké výsledky ste dosiahli.

Hodnotenie (15 bodov):

- PDF dokumentácia výsledkov a zistení - správa je nutnou podmienkou k hodnoteniu zadania. Program musí byť tiež funkčný.
- 4b za rozlúštenie krátkeho kryptogramu.
- 2b za získanie permutácie k transpozičnej časti.
- 3b za dešifrovanie transpozície.

- 6b za dešifrovanie jednoduchej substitúcie.

Posledná zmena: Monday, 13 December 2021, 21:10

◄ Kryptoanalýza II

Ísť na...

Kostra aplikácie ►