Rotating Grille

Cardano Girolamo Cardano invented: Fleissner, after Austrian cryptologist (Eduard). Described by Jules Verne in the story Mathias Sandorf.

An even number of cells on each side of grille square. Clip out 1/4 of them at random so they don't conflict. (not hard... cute exercise p. 27).

OR use a Key!. Anyway... grille has tab that points NESW say, at four stages of encipherment. for 6x6 grille, have 9 letters per direction. write them into the holes with grille pointing N, then E, then S, then W. L to R, top to bottom. Variants: obvious. use NSWE or write in in different pattern.

Decipher obvious?

The strictly horizontal writing-in has to obey some rules: 9 letters out of 36 means they're 4 apart on the average, so if some are farther, others are closer. Further, for each letter, there are three others that COULD NOT have been written in in the same minor unit with it, and you know just where and what they are. ALSO you know that position S is N reversed, as with E and W. So once you have a digram or possible word in one position you can check it out by seeing what happens in the opposite direction in the reverse grille position (or if your imagination is good enough, the other 2 positions as well).

So if you have

```
BTMRXU
VCIAIS
RFDUSU
TIRIHE
INONCS
TOJSON
Number cells
123456
789...
```

and you have prob. word VIADUCT, good! only one V, near the top at 7 so you'd expect IAD..in same unit. So note that cells 5, 30, and 32 weren't used in this grille position since that's where 7 rotates to. Next, there are lots of I's but only one A, which has to come after the I, so we're rolling. rotate, cross out...

D kills off one of the remaining U's as well. We have some "holes" in the grille, and if we reverse them and read out what's underneath in regular order we get TIONS. Wow! VIADUCT goes to UCTIONS.

W/o a word, use probable di- or trigrams.

or....

```
 1  2  3  4  5  6 ...
 B  T  M  R  X
 N  O  S  J  O
36 35 34 33 ..
```

so notice that TR (24) gives JO (33 35). Note can't choose conflicting pairs (like 16) for digrams!... won't be uncovered at same time. There are more or less mechanical ways (paper strips!) to attack, but this is all we need for Zurbia.

Substitution

Read the Gaines chapter linked from syllabus.

Main types are Simple (Monoalphabetic) and Polyalphabetic.

Statistical attack on affine cipher

- Compile tables of frequencies of individual ciphertext characters
- Use these to guess at ciphertext characters that represent two common plaintext characters, say, e and t
- Use these guesses in formula for known plaintext attack (since in our encoding, t - e = 19 - 4 = 15, relatively prime to 26, with inverse 7, this should work)
- Check tentative decoding. If gibberish, make another guess.

- Note that if t - e were even or 13, than attack would not work. Suggests that encryption could be made robust against this attack by re-organizing the alphabet so that all common letters have even indices.

Basic Statistical Attack Substitution Attack

Somewhat less structured, with more trial and error, than for affine, but generally can be made to work, even without word boundaries, for long enough messages (above 100-200 characters, or even longer than about 25 if you are really good). Also special methods for short ciphers, using WORD frequencies (ACM article). Basic attack known to Arabs by 9th century AD, rediscovered in Europe in 15 century.

- Compile tables of frequences
- Guess a ciphertext characters for few most common chars, say e, t, and a.
- Use these guesses to look for common trigrams with two of the letters (the, tha, hat, ... and check consistancy of guesses)

- Once this looks right, use similar approach to find encodings of next few most common letters (o,i,n -¿ ing, and, ion, ...)
- At this point, enough partial english words should start to pop out, that remainder of decoding process is relatively simple word puzzle.
- Numerous variations on 2-4 can be employed, some using bigrams instead of, or in addition to trigrams.

One fairly effective counter to above attack is "Homophonic subsitution" where several symbols are used for each letter, with more common letters getting more codes in proportion to frequency. Removes single-character information, and forces attack to start at level of bigrams. Of course key is also longer, and harder to change.

Advanced Substitution Decipherment

- Frequencies (single, di, tri)
  ETAIONSHRDLU
- Contact Chart – Only do for common letters (after freq). AEIO are normally high-freq. letters contacting lo-freq letters are often vowels letters with wide variety of contact are often vowels in repeated digrams, one letter usually a vowel.
- common words advanced technique – check its expected letter frequencies against all positions in the cryptogram for match against cryptogram's real freqs.
- Common patterns XYZZZAABBC, or XYZ and XYQX or XYYZ etc. etc.

Advanced Substitution Attack Cont.

- Word divisions!
- Terminal sequences (-ions, -ed,), along with prefixes (in-, ex-) and short words (to, in, is)
- Vowel ID
- MULTIPLE ANAGRAMMING! Very General Trick!
- Just find an entry! anything.