MATH2068/2988
Number Theory and Cryptography
Week 3 Lecture 2

Robert Howlett, ed. Anthony Henderson, Dzmitry Badziahin

The University of Sydney

15th August 2017

Transposition ciphers

All the classical cryptosystems in yesterday's lecture were of the type called *substitution ciphers*, where each letter (or block of letters) in the plaintext is replaced by another according to some rule, but the ordering is unchanged. In a *transposition cipher*, the letters are unchanged but they are put in another order.

So if the plaintext is $c_1 c_2 \dots c_N$ then the ciphertext is $c_{\pi(1)} c_{\pi(2)} \dots c_{\pi(N)}$, where π is some permutation of the numbers $1, 2, \dots, N$.

This looks very secure because there are $N!$ different permutations of $1, 2, \dots, N$. Moreover, the frequency of individual letters is not changed, so letter frequency analysis is pointless. But unless the length of all messages is fixed in advance, the permutation π will have to be determined by some smaller rule; and it may then succumb to digraph or polygram frequency analysis.

An example of a transposition cipher

One simple procedure is to write the input message along the rows of a rectangular array, and obtain the output message by reading down the columns.

A U S T R A L I
A N S A L L L E
T U S R E J O I
C E F O R W E A
R E Y O U N G A
N D F R E E

The ciphertext, split into blocks of length 5 for convenience, would be AATCR NUNUE EDSSS FYFTA ROORR LERUE ALJWN ELLOE GIEIA A.

The width of the array serves as the key both for encryption and decryption. To decrypt knowing the key, use the total length of the message to figure out the length of the short last row, and then enter the cipher text into the columns.

Block transposition ciphers

Another system involves splitting the message into blocks of some fixed size m and rearranging the letters within each block according to some permutation of $\{1, 2, \dots, m\}$. We call this a *block transposition cipher*; the permutation of $\{1, 2, \dots, m\}$ is the key.

For example, suppose the block length is six and the key is 634125.

(This means that in each block the 6th letter of the input message becomes the first letter of the output, the third of the input becomes the second, and so on.)

Plaintext: ENCRYPTIONANDDECRYPTIONSHOULDBEEASYIFYOUKNOWHOW

ENCRYP TIONAN DDECRY PTIONS HOULDB EEASYI FYOUKN OWHOW*
PCRENY NONTIA YECDDR SIOPTN BULHOD IASEEY NOUFYK *HOOWW

Ciphertext: PCRENYNONTIAYECDDRSIOPTNBULHODIASEEYNOUFYKHOOWW

Finding the block length

Suppose an eavesdropper intercepts the ciphertext $c'_1 c'_2 c'_3 \ldots c'_N$. Noticing that the letter frequencies are as in ordinary English, they may suspect a block transposition cipher. To decipher it, they will first need to find the block length m. They could test the possibilities $m = 2$, $m = 3$, etc. as follows.

For each possible block length m, examine the $[k, \ell]$-*decimation of M' of period m* for various values of k and ℓ in the range $\{1, 2, \ldots, m\}$. This is the following sequence of pairs:

$$\mathrm{Dec}([k, \ell], m) = [c'_k c'_\ell,\ c'_{k+m} c'_{\ell+m},\ c'_{k+2m} c'_{\ell+2m},\ c'_{k+3m} c'_{\ell+3m},\ \ldots].$$

The idea is that if m is the block length, and if c'_k and c'_ℓ were adjacent letters in the plaintext – say $c'_k = c_n$ and $c'_\ell = c_{n-1}$ – then c'_{k+qm} and $c'_{\ell+qm}$ would also have been adjacent in the plaintext, for all values of q.

Then the frequency distribution of the pairs in $\mathrm{Dec}([k, \ell], m)$ should match the typical frequency distribution of *digraphs* (adjacent pairs of letters) in normal unencrypted text.

Finding the block length (continued)

A quick test to see if the distribution might be right is to compute the coincidence index for $\mathrm{Dec}([k, \ell], m)$.

For each pair of letters ij we let p_{ij} be the relative frequency of ij in $\mathrm{Dec}([k, \ell], m)$. That is, p_{ij} is the number of occurrences of the pair ij in the sequence divided by the length of the sequence. Then the CI (coincidence index) is $\sum_{ij} p_{ij}^2$. This is the probability that two randomly chosen pairs in the decimation are the same.

A random sequence of letters will have digraph coincidence index near the lower bound of $(1/26)^2 \approx 0.0015$. Ordinary English text has ≈ 0.007 or more.

So, starting at $m = 2$, compute the CI of $\mathrm{Dec}([1, \ell], m)$ for all ℓ from 2 to m. If some ℓ gives CI ≥ 0.007, then m is a good candidate for the block length; otherwise, move on to the next possible m.

Coincidence discriminant

Another statistic one can use instead of or as well as the digraph CI is the *coincidence discriminant* (CD).

For each letter i define $p_{i\_}$ to be $\sum_h p_{ih}$, the relative frequency in $\mathrm{Dec}([k, \ell], m)$ of pairs that begin with i.

And define $p_{\_j}$ to be $\sum_h p_{hj}$, the relative frequency in $\mathrm{Dec}([k, \ell], m)$ of pairs that end with j.

The CD is defined to be $\sum_{ij} (p_{ij} - p_{i\_} p_{\_j})^2$.

If the event that a randomly chosen pair in $\mathrm{Dec}([k, \ell], m)$ starts with i and the event that it ends with j are roughly independent of each other, then p_{ij} will roughly equal $p_{i\_} p_{\_j}$. So for random text the CD should be very close to 0.

But if ij is a very common or very uncommon digraph then $(p_{ij} - p_{i\_} p_{\_j})^2$ will be noticeably positive. In fact, the CD is reliably ≥ 0.003 for normal text.

Finding the key knowing the block length

If m is known to be the block length, compute the CI and/or the CD of $\mathrm{Dec}([k, \ell], m)$, for all k and ℓ.

Large values of the CI (say ≥ 0.007) and large values of the CD (say ≥ 0.003) suggest that c'_k and c'_ℓ were adjacent in the plaintext. By finding the most likely adjacencies one can figure out how to reorder the letters in each block to recover the plaintext.

Actually the CI and the CD tell you only if the two letters in question were (probably) adjacent, they don't tell you which is first and which is second. So you are just as likely to come up with the reverse of the correct order as the correct order. But it is easy to try both.

§5 Euler - Fermat Theorem.

§5.1. More on Reduced Systems of Residues.

Proposition. Let $a, b, d \in \mathbb{Z}$, $d \geq 2$.
If $d \mid ab$ and $\gcd(a, d) = 1$ then $d \mid b$.

Proof By EEA, $1 = s \cdot a + t \cdot d$ for $s, t \in \mathbb{Z}$.

$$\Rightarrow b = \underbrace{s\,ab}_{\text{multiples of } d} + \underbrace{t \cdot d \cdot b}_{\text{multiples of } d} \Rightarrow d \mid b$$

☒

Proposition. Let $a, b, m \in \mathbb{Z}$, $m \in \mathbb{Z}^+$ such that $\gcd(a, m) = \gcd(b, m) = 1$. Then $\gcd(ab, m) = 1$

Proof. Assume $\gcd(ab, m) = d > 1$.

$d \mid m$, $\gcd(a, m) = 1 \Rightarrow \gcd(a, d) = 1$.

$d \mid ab$, $\gcd(a, d) = 1 \Rightarrow$ [Proposition]
$\Rightarrow d \mid b \Rightarrow \gcd(b, m) \geq d > 1$
Contradiction

☒

The last proposition suggests that we can define multiplication in reduced systems of residues mod m

Examples: $m=8$ $m=10$

X	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

X	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

For each element a in a reduced set we have its inverse $a^{-1} \pmod m$ inside the set.

§7.2 Euler, Fermat Theorem.

Proposition: Let R be a reduced system of residues mod m. Let $a \in \mathbb{Z}$ with $\gcd(a, m) = 1$. Then

$$aR := \{ar : r \in R\}$$

is also a reduced system of residues mod m.

Proof. Firstly show that elements of aR are pairwise non-congruent.

$$ar_1 \equiv ar_2 \pmod m \Rightarrow r_1 \equiv r_2 \pmod m$$
$$\Rightarrow r_1 = r_2.$$

Also $\gcd(ar, m) = 1$ for any $r \in R$ by the proposition.

Finally, aR contains exactly one representative for each invertible congruence class mod m $\Rightarrow$ aR is a reduced system ☒

(Ex: The same applies to complete systems of residues: if $\gcd(a, m) = 1$ then aR is a complete system of residues)