Recall: Kasiki's Test.

- I AM THE BEST AT THE GAME.
  BAG BAGB BAGBAG BAG BAGB

Encrypted using the key BAG

Here THE gets encrypted the same twice in the text.

THE occurs at positions 4 and 13. 13-4=9.
So key length is "likely" a divisor of 9.

Summary:

- Find triples (or quadruples or ...) of repeated letters in the encrypted text.
- Take the differences in their starting positions.
- Note that words that are multiples of the key length apart get encrypted the same way. So by taking the gcd of the numbers from the previous step, you get a guess at the key length.

Q: How do we know the key length is correct? We can also verify this using the index of coincidence.

Index of Coincidence: How likely two random letters coincide.

In English, $IC \approx 0.065$. (much better than random).

Given an encrypted string, how do we compute this value?

Let f_0 be the frequency of A's in the string, f_1 be the frequency of B's in the string, ... f_{25} be the frequency of Z's in the string.

For each letter, we get $\binom{f_i}{2} = \frac{f_i(f_i-1)}{2}$ ways to pick two letter "i"s.

Total number of ways to pick two letters from one $\binom{n}{2} = \frac{n(n-1)}{2}$ where n is the string length. Thus.

$$IC = \frac{\sum_{i=0}^{25} \frac{f_i(f_i-1)}{2}}{\frac{n(n-1)}{2}} = \frac{\sum_{i=0}^{25} f_i(f_i-1)}{n(n-1)}$$

If IC is around 0.065 (or bigger) then you have found a VERY likely key length.

Exponentiation Ciphers.

Throughout let $p > 2$ be a prime and e the encryption key. We require that $\gcd(e, p-1) = 1$.

Encryption is done as follows:

1. Encrypt our letters one by one according to A=00, .. Z=25.
2. Group the digits together in blocks of size $2m$ where

$$\underbrace{2525\ldots25}_{m \text{ copies of } 25} < p < \underbrace{252525\ldots25}_{m+1 \text{ copies of } 25}.$$

This ensures that we get the most out of p and avoid collisions. (for example, if $p = 2633$ then $m = 2$ since $2525 < 2633 < 252525$. Possibly pad the ending with X's to get even blocks of $2m$.

3) For each block P of size $2m$ decimal digits, encrypt as

$$C \equiv P^e \bmod p \qquad 0 \le C < p.$$

4) The collection of numbers is the encrypted message. Do NOT convert back to letters (it will usually be impossible to do so).

Ex: Using $p = 2633$ and $e = 29$ (note $\gcd(29, 2632) = 1$), encrypt

THIS IS AN EXAMPLE OF AN EXPONENTIATION CIPHER.

Soln:

Since $2525 < p < 252525$, we group in blocks of $n = 2$.

Write our numbers using the table.

1907	0818	0918	0013	0423
0012	1511	0414	0500	1304
2315	1413	0413	1908	0019
0814	1302	0815	0704	1723

↳ X.

Encrypt each block using

$$C \equiv P^{29} \mod 2633.$$

Eg. $1907^{29} \equiv 2199 \mod 2633$ (use Sage).

$(818)^{29} \equiv 1745 \mod 2633$

⋮

Encrypted text is

2199	1745	1745	1206	2437
2425	1729	1619	0935	0960
1072	1541	1701	1553	0735
2064	1351	1704	1841	1459.

P = Plaintext.

To decrypt, compute the inverse of $e \bmod p-1$ (THAT'S WHY we need $\gcd(e, p-1) = 1$) (In other words) find d such that

$$de \equiv 1 \bmod p-1 \quad \text{so } de = 1 + k(p-1) \text{ for some } k.$$

If $C = 0$ then $P = 0$ so assume $\gcd(C, p) = 1 = \gcd(P, p)$ Then to decrypt, compute $C^d \bmod 2633$.

This works since (Recall $C \equiv P^e \bmod 2633$)

$$C^d \equiv (P^e)^d \equiv P^{ed} \equiv P^{1+k(p-1)} \equiv P \cdot P^{k(p-1)} \equiv P \cdot (P^{p-1})^k \bmod p.$$

$$\equiv P \cdot 1^k \bmod p$$

(Euler's theorem OR Fermat's Little Theorem)

$$\equiv P \bmod p.$$

$d=10$ $\cdot 3 \cdot 10 \equiv 1 \bmod 29$

Ex: $p=29$, $e=3$. TO BE OR NOT TO BE

B $(01)^3 \equiv 1 \bmod 29$

E $(04)^3 \equiv 64 \equiv$ [illegible] $4+60 \equiv 4+2(30) \equiv 4+2(1) \equiv 6 \bmod 29$

N $(13)^3 \equiv 169 \cdot 13 \equiv (5 \cdot 30+19) \cdot 13 \equiv 24 \cdot 13 \equiv (-5)13 \equiv -65 \equiv -2(30)-5 \equiv -2+24 \equiv 22 \bmod 29$

O $(14)^3 \equiv (13+1)^3 \equiv 13^3+3 \cdot 13^2+3 \cdot 13+1 \equiv 22+324+$
$\equiv 2^3 \cdot 7^3 \equiv 8 \cdot 49 \cdot 7 \equiv 8 \cdot 20\ 7 \equiv 20 \cdot 56 \equiv 20(-2) \equiv -40 \equiv 18 \bmod 29$

[illegible]R $(17)^3 \equiv (-12)^3 \equiv -2^6 \cdot 3^3 \equiv -64 \cdot 27 \equiv -64(-2) \equiv 128 \equiv 70 \equiv 12 \bmod 29$

T $(19)^3 \equiv (-10)^3 \equiv -1000 \equiv 1900 \equiv 1800+100 \equiv 60(30)+100 \equiv 160 \equiv 150+10$
$\equiv 5(30)+10 \equiv 15 \bmod 29$

15, 18, 1, 6, 18, 12, 22, 18, 15, 15, 18, 1, 6.