**Exponentiation Ciphers**

Exponentiation ciphers are more resistant to cryptoanalysis.

Let $p$ be an odd prime and let $r \in \mathbb{N}$ with $(r,\, p-1) = 1$ be the *enciphering key.*

To encipher,

(1) transform letters to two digit numbers:

| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 00 | 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

;

(2) group the resulting numbers into blocks of $2m$ digits, where $m$ is the largest natural number such that any $2m$ digit number which could appear is less than $p$ (for example, if $2525 < p < 252525$ then $m = 2$);

(3) for each plaintext block $x$, an integer with $2m$ digits, form a ciphertext block $y$ by taking $y \in \overline{\mathbb{N}}$ with $0 \le y < p$ satisfying

$$y \equiv x^r \pmod{p}\,.$$

To decipher, we need the *deciphering key* $r'$, which is the inverse of $r$ modulo $p-1$, i.e.

$$rr' \equiv 1 \pmod{p-1}\,.$$

Indeed, it follows that there exists $k \in \mathbb{Z}$ such that $rr' = 1 + k\,(p-1)$. Hence, by Fermat's Theorem 14.8,

$$\begin{aligned} & y \equiv x^r \pmod{p} \\ \Rightarrow\ & y^{r'} \equiv x^{rr'} \pmod{p} \equiv x^{1+k(p-1)} \pmod{p} \equiv x \cdot \left(x^{p-1}\right)^k \pmod{p} \equiv x \pmod{p}\,. \end{aligned}$$

So $x \equiv y^{r'} \pmod{p}$.

**Examples 16.6.** (1) Consider $p = 29$ and $r = 3$ . Then $(r,\, p-1) = (3,\, 28) = 1$, $m = 1$ and $r' = 19$. Hence we have that

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | T | H | I | S | E | X | A | M | P | L | E |
| $\rightarrow$ | 19 | 07 | 08 | 18 | 04 | 23 | 00 | 12 | 15 | 11 | 04 . |
| $\rightarrow$ | 15 | 24 | 19 | 03 | 06 | 16 | 00 | 17 | 11 | 26 | 06 |

For example, for $x = 11$

$$11^2 = 121 \equiv 5 \pmod{29} \;\Rightarrow\; x^r = 11^3 \equiv 55 \pmod{29} \equiv 26 \pmod{29} \;\Rightarrow\; y = 26.$$