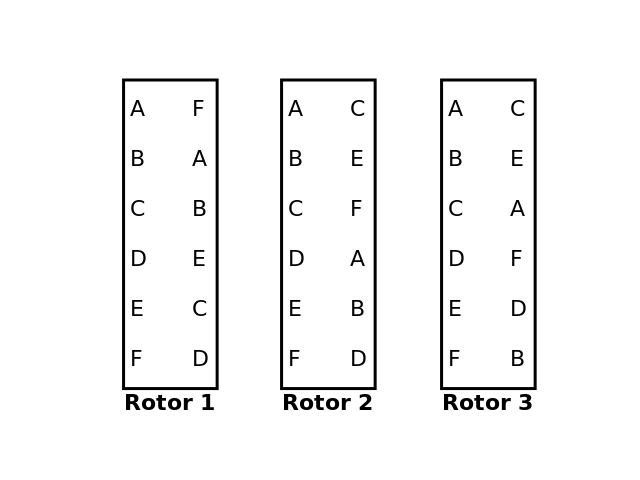
انیگما یک ماشین رمزنگاری است

مدل آن به شرح زیر کار میکند:



1

وقتی به عنوان مثال دکمه

(a)

میزنیم به ترتیب از ستون چپ به راست این فراند انجام میشود

1 A->F -> 2 F->D -> 3 D-> F

2

در نهایت این حرف انتخابی به یک رفلکتور وارد میشد که دارای حروف الفبا به ترتیب بود و از این مرحله یک حرف الفبا به صورت زیر انتخاب میشد:

مثال:

a->z

b->y

x->c

3

بعد این مرحله مطابق مرحله یک هر حرف معادل روبه رویی آن انتخاب میشود

مثال:

3 A-> c -> 2 c->a -> 1 a-> b

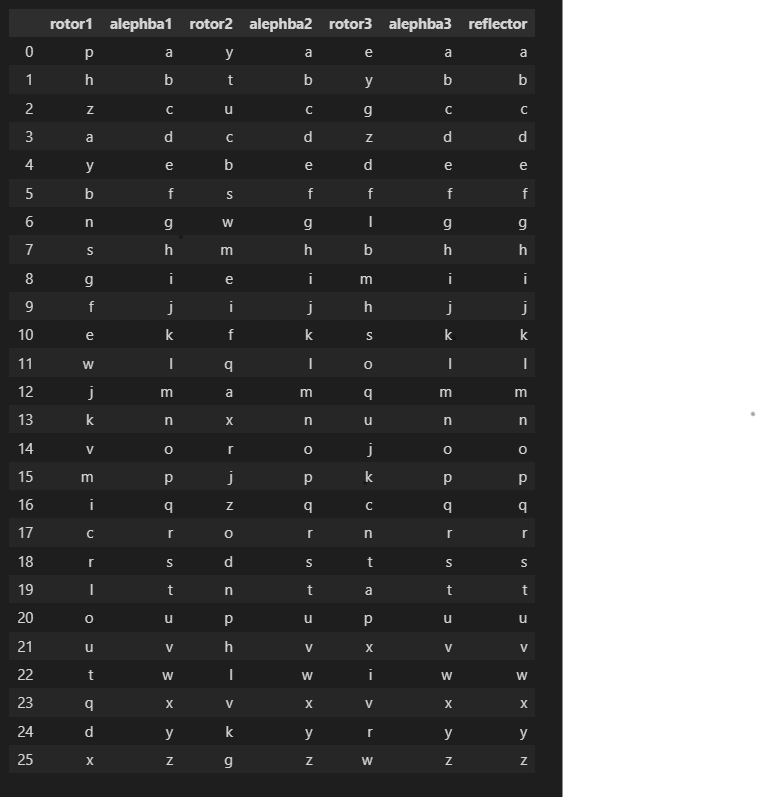
4

وقتی یک کلمه رمز شد و این فرایند یکبار تکرار شد روتور یک ستون اول آن یکبار میچرخید که مثلا حرف (f) در جایگاه آخر روتور می آمد و حرف(d) در جایگاه اول

هر 26 بار که روتور یک میچرخید نوبت روتور دومی میشد که آن هم 26 بار

میچرخید نوبت روتور 3 میشد که ان هم در نهایت 26 بار میچرخید

Machine\_enigma



Example:

:رمز1 a->d 2 d->s 3 s->k -> 3 p->k 2 k->f 1 f->b a:b

شکستن رمز: b:a

5

در واقع اگر یک نفر میخواست که رمز را بخواند و بشکند باید حتما سیستم ماشین خود یا همان روتور های خود را مطابق با ماشین رمز کننده تنظیم میکرد و بعد رمز را درون ماشین خود وارد کند تا پیام اصلی را دریافت کند

:رمز a:b

شکستن رمز: b:a