VE475 Review

Anna

第一章

various ciphers

1. Casear cipher：将每一个字母移动N个
2. One time pad：$n \oplus k = C$

gcd, prime 的关系

a coprime with b : $\gcd(a,b)=1$

$\Rightarrow as+bt=1$

$\Rightarrow as \equiv 1 \bmod b$

$\Rightarrow$ a and s is inverse mod b