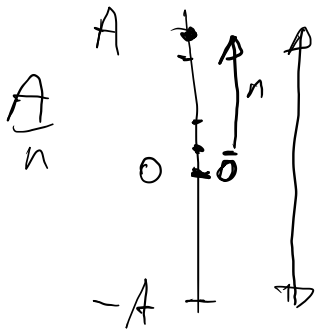
erreur

valeur



$2n+1$

$\frac{T}{1000}$

L $\frac{1}{0}$

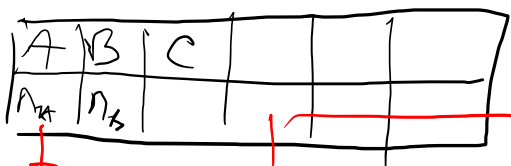
$1 - \frac{L}{T}$

$\frac{999}{1000}$

$M = A\ A\ B\ B\ A\ A\ C\ C \ldots$ → n

1) voc

freq



2)

3) $P_A = \frac{n_A}{S}$ $\frac{n_X}{S}$ ⋯⋯⋯→

4) $H(M) = -\left(P_A \log(P_A) + P_B \log(P_B) \cdots + \right)$

$\log_2(x) = \frac{\log(x)}{\log(2.0)}$

$$H(M) = -\sum_{i=0}^{t} p_i \log p_i$$

$t = |V|$

le chat $p(x_i | x_{i-1}, \ldots)$

privé d

public e_A, n_A

privé

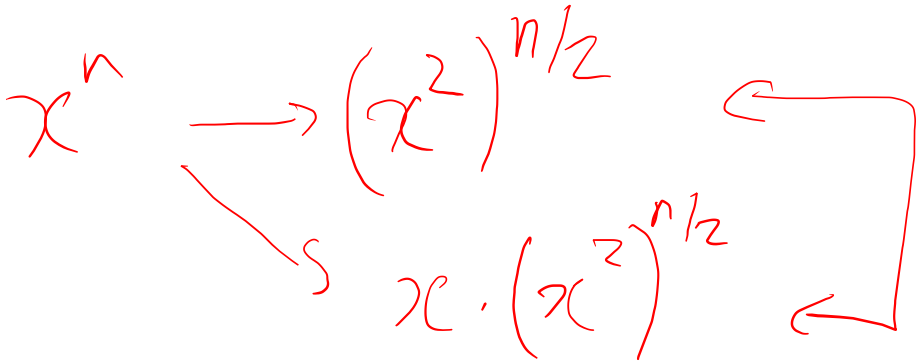
public (e_B, n_B)

A → confidentialité → B

M → (responsabilité) signer →

$$\left(S = M^{d_A} \bmod n_A\right)^{e_B} \bmod n_B$$

$$(M^e)^d \qquad M^{ed} = M \bmod n \qquad (M^d)^e$$



$3713^{158} \bmod 5837$

$2^2 \bmod 3732$

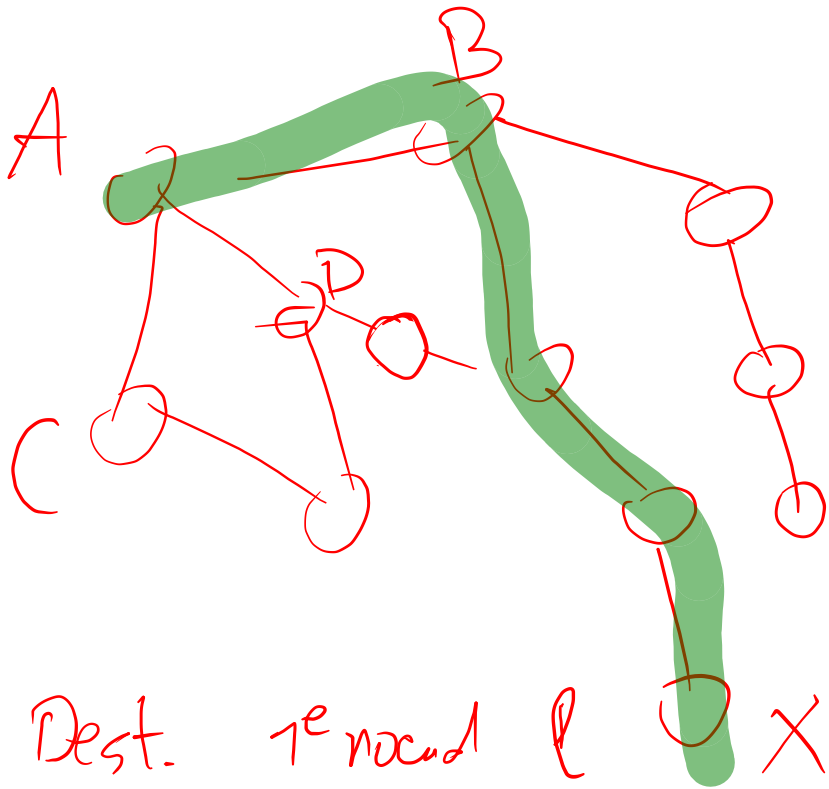
$3^4 = 2 \bmod 79$ $3^{(5)} \bmod 79$

$3^2 = 9$

$9^2 = (81)$

$x^y \bmod z$

```
exp( int x, int y, int z )
{
    if (y == 1)
        return x % z;
    else if (y % 2 == 0)
        return exp((x * x) % z, y / 2, z) % z;
    else
        return (x * exp((x * x) % z, y / 2, z)) % z;
}
```



pour A

Dest.	1e nœud	l
X	B	4