Small e

To encrypt quickly use small e .
(corresponding d is large)

Typical suggestion is $e = 2^{2^4} + 1 = 65{,}537$
encryption takes 17 mult.

For simplicity we take $e=3$
as an example.

Problem:

Given $C=M^3$ *(mod N)* find M.

Underlying Theorem

Theorem (Coppersmith):

Let $p(x) = 0 \pmod{N}$

be a polynomial equation of degree d.

Then can efficiently find all solutions

x_0 satisfying $|x_0| < N^{1/d}$

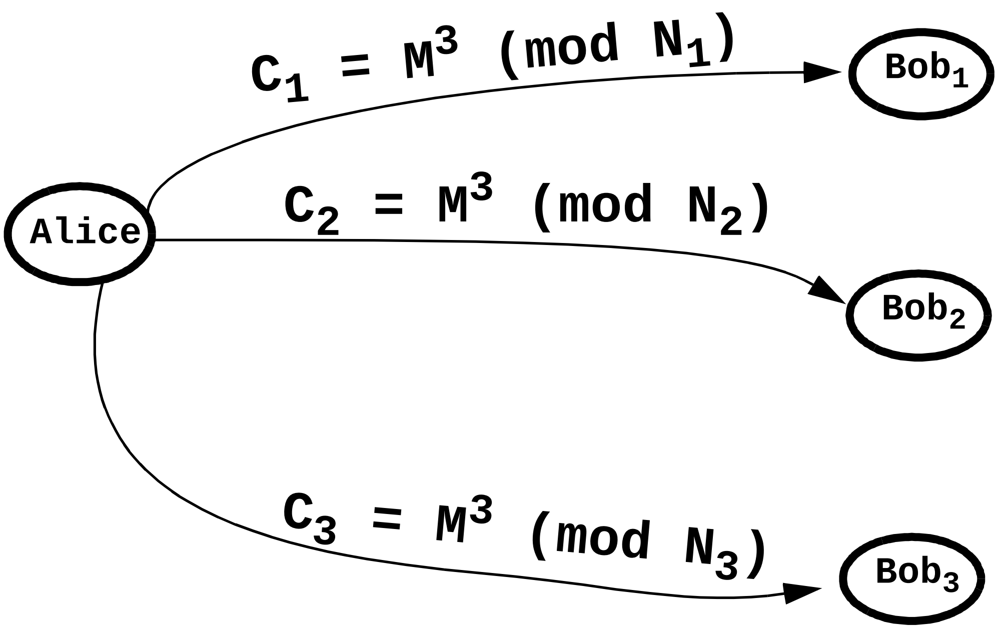
Remark: Suppose $p(x) = x^d - c \pmod{N}$

Then theorem is trivial.

The remark suggests that the theorem cannot be improved.

Broadcast Attack

Blum, Liebherr, Williams:



Given C_1, C_2, C_3 Eve can find M.

CRT

Chinese Remainder Theorem (CRT):

Assuming $\gcd(N_i, N_j)=1 \quad 1 \le i < j \le 3$

there exists a unique $\quad 0 \le X < N_1 N_2 N_3$

such that

$$X = C_i \quad (mod\ N_i) \quad \text{for} \quad i=1,2,3.$$

X can be efficiently constructed.

Claim: $X = M^3 \quad (mod\ N_1 N_2 N_3)$

But, $M^3 < N_1 N_2 N_3$ so $X = M^3$.

$\Rightarrow$ Given X can easily find M.

Franklin-Reiter

$M_1 =$	`text`	`s`
$M_2 =$	`text`	`s+1`

Suppose Eve intercepts two ciphertexts:

$$C_1 = M_1^3 \quad \text{and} \quad C_2 = M_2^3 \quad (mod\ N)$$

where $M_2 = M_1 + \Delta$ and Δ known.

M_1 is a common root of the polynomials:

$$f_1(X) = X^3 - C_1 \quad \text{and} \quad f_2(X) = (X+\Delta)^3 - C_2$$

Eve can recover "**`text`**" by computing

$$gcd(f_1, f_2) = \text{“}X - M_1\text{”} \quad (mod\ N)$$

Unknown Δ

$M_1 =$	**`text`**	**r_1**	**`random pad`**
$M_2 =$	**`text`**	**r_2**	

$M_2 = M_1 + \Delta$ where Δ is <u>unknown</u>.

Set $C_1 = M_1^3$ and $C_2 = M_2^3 \quad (mod\ N)$

$f_1(X) = X^3 - C_1$ and $f_2(X,Y) = (X+Y)^3 - C_2$

have a common root when $Y=\Delta$.

$\Rightarrow$ Δ is a root of $g(Y) = \mathrm{Res}_X(f_1, f_2)$.

$g(Y)$ has degree $e^2 = 9$.

$\Rightarrow$ as long as $\Delta < N^{1/9}$ Eve can find Δ !!

Then use Franklin-Reiter to find "**`text`**"

Timing Attack

Attack (Kocher):

Measuring the time it takes to compute $C^d \ (mod\ N)$ for many C can reveal the secret d.

Repeated squaring: $d = d_n\, d_{n-1} \ldots d_1\, d_0$

$A \leftarrow 1$	$Z \leftarrow C$
$A \leftarrow A \cdot Z^{d_0}$	$Z \leftarrow Z^2$
$A \leftarrow A \cdot Z^{d_1}$	$Z \leftarrow Z^2$
$A \leftarrow A \cdot Z^{d_{n-1}}$	$Z \leftarrow Z^2$
$A \leftarrow A \cdot Z^{d_n}$	

Timing attack (cont.)

d odd implies $d_0 = 1$

Messages: $C_1,\ C_2,\ C_3,\ \ldots,\ C_k$

Times: $T_1,\ T_2,\ T_3,\ \ldots,\ T_k$

Time for $C_i \times C_i^2 \ (mod\ N)$:

$t_1,\ t_2,\ t_3,\ \ldots,\ t_k$

If $d_1 = 1$ then

the random variable T and t
are correlated.

Otherwise, they are “independent”.

Iterating this reveals the bits of d .