

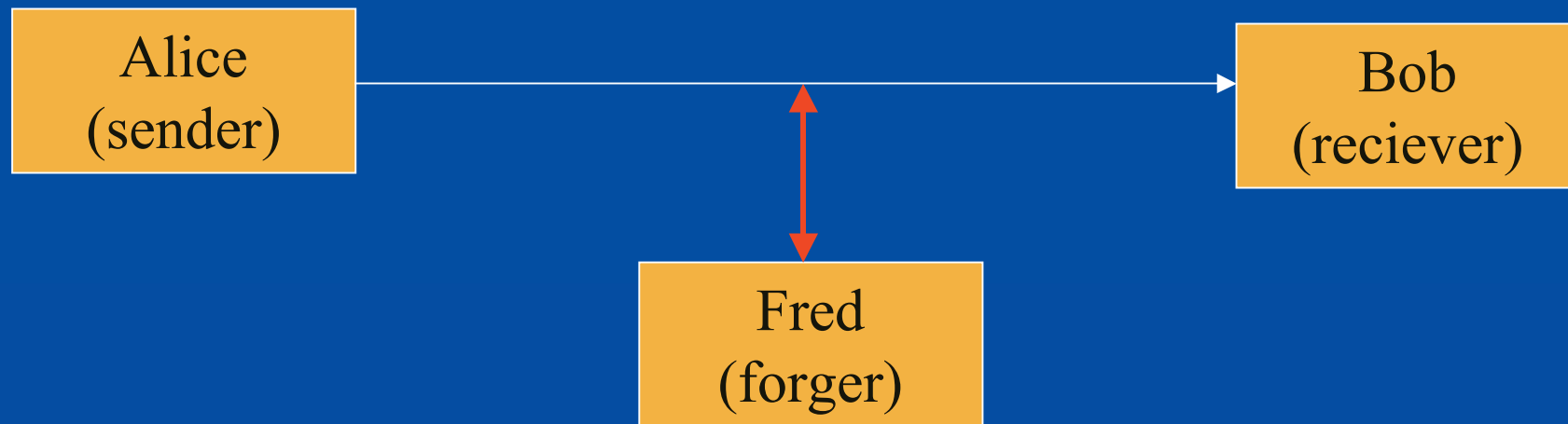
# Introduction to Modern Cryptography

## Lecture 6

1. A Clarification regarding CBC MACs.
2. Chinese Remainder Theorem (at long last).
3. Testing Primitive elements in  $Z_p$
4. Primality Testing.
5. Integer Multiplication & Factoring as a One Way Function.

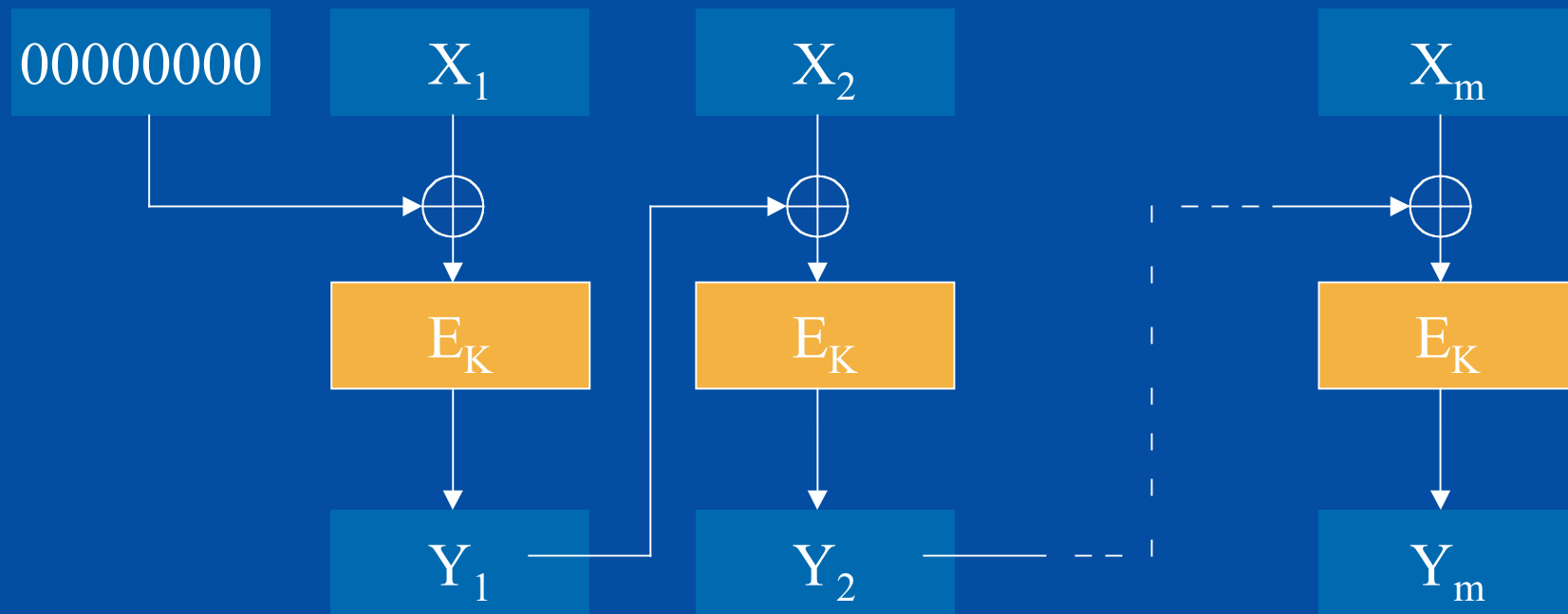
# Reminder: MACs

Ensure *integrity* of messages, even in presence of an *active* adversary who sends own messages.



Remark: *Authentication* is orthogonal to *secrecy*, yet systems often required to provide both.

# Reminder: CBC MAC<sub>K</sub>



$$\text{CBC-MAC}_K(X_1, X_2, \dots, X_m) = Y_m$$

# Clarification: Security of CBC MAC

**Claim** [Bellare, Kilian, Rogaway]:

If  $E: \{0,1\}^k \times \{0,1\}^n \rightarrow \{0,1\}^n$  is a pseudo random function, then CBC MAC is resilient to adaptive existential forgery.

Proof of security applies only to fixed number of blocks  $m$  (e.g.  $m=17$  or  $m=n^2+51$ ).

Proof is inapplicable to variable length  $m$  (as discussed in Problem Set II).

# Adaptive Existential Forgery

1. Forger picks  $message_1$  , gets  $MAC_K(message_1)$
2. Forger picks  $message_2$  , gets  $MAC_K(message_2)$

·  **adaptive**

3. Forger picks  $message_s$  , gets  $MAC_K(message_s)$

Now forger should come up with any new pair

$new\_message, MAC_K(new\_message)$

 **existential**

# The Chinese Remainder Theorem (CRT)

# Testing Primitive Element mod $p$

Let  $p$  be a prime number so that the prime factorization of  $p-1$  is known:

$$p-1 = q_1^{e_1} q_2^{e_2} \dots q_k^{e_k} \quad (q_1, q_2, \dots, q_k \text{ primes}).$$

Theorem:  $g \in \mathbb{Z}_p$  is a primitive element in  $\mathbb{Z}_p$  iff  $g^{(p-1)/q_1}, g^{(p-1)/q_2}, \dots, g^{(p-1)/q_k}$  are all  $\neq 1 \pmod p$

Algorithm: Efficiently compute all  $k$  powers.

Caveat: Requires factorization of  $p-1$ .

# Testing Primitive Element mod p

```
> isprime(2^229-91);  
true  
> p:= 2^229-91;  
p := 862718293348820473429344482784628181556388621521298319395315527974821  
> a:= (p-1)/2 :  
> 3^a mod p;           # naïve exponentiation  
Error, integer too large in context      # infeasible  
> 3 &^ a mod p;  
1      # thus 3 is not a primitive element mod p  
> verify (6 &^ ((p-1)/2) mod p , 1, equal);  
false  
> ifactor(p-1,easy);           # the “easy to get” factors of p-1  
(2)2 (3)5 (5) (3143029) (40591) c-55-1
```

# Testing Primitive Element (cont.)

```
> p:= 2^229-91:      # 2,3,5,40591,3143029 are the easy factors of p-1
> verify (6 &^ ((p-1)/3) mod p , 1, equal);
      true          # thus 6 is not a primitive element mod p
> FactorsList:={2,3,5,40591,3143029}:
> g:=233926:
> for q in FactorsList do
> print(q,verify(g &^ ((p-1)/q) mod p,1,equal)); od;
      2,false
      3,false
      5,false
      40591,false
      3143029,false
```

So far, **233926** looks like a good candidate (it passed all five tests it went through). However, we cannot know for sure without factoring the remaining  **$c-55-1$**  (which is not a prime).

# Primality Testing

## A PRIME FOR THE MILLENNIUM

1695622712880687478874003932225733145418  
7103117215258402822754639444439150176651  
87677648590458200095276019439238167628964  
4727216145060104767560592095535299114691  
2809889393788383275988559054911295888721  
82960597685441916678707336381948421313108  
6251607398289162598493809031710972006227  
445253342228076766180550265759472807075176  
84719662198217315344351220000523695481076  
0431933960890325207991357855479116978257  
2481377092146219144800411212411986131890  
3084696307908851821381356953026591660917  
7557080415453180322286256899342813720132935  
6540456101231353607074556964820520111191  
7803917089426925046726225659955364931026  
1669288943925646787558249168656785250545  
2615238453748481731189917697254592971701  
94389891282683509781988688634535632050868  
5864934342407483040664864199146135944131  
2447494379322488285783808178719040181648  
61392979973303392716886500570778220506278  
5523328058642568203317669603421099129748074  
2931674802805786249535420221209942941757  
6968655166743180824969651582473388052430  
23076327322846854292869718923971577651169  
2379905048712275705407112403614798424206  
0317055743215346402267587221808345889464  
8590077982826550431634699098451988007731  
48443020688273674603490411264380530557953  
6776436596545370995982233304571888022964  
36148103186029822732858048652060292146971  
6777408128905357283769843138458373316316  
8315320866788978732054662757387113620757  
1175888111339396758758911092609299362282  
6554868172778946611292164358541457015429  
8104289971895529671817718760720047296316  
5719294795405350204397359590266932837619  
4266972486325762812319235317644619299197  
8366133934267987429040830567754122294457  
1332463609098549099900518313145113955639  
57356654879738202927885880243930464615895  
0266071940448366958466636932720958627072  
0473060427975493713476058004161080839413  
7312623865116223810625427962816045901699  
1526332735165194734663597772286383643625  
3025277745695134127559388639742683165558  
5085243207960204791349952790055068921915  
2703706763849942067841781864906059067455  
90283452037983466078222008724593604204628  
5093059704977817748127777709652208140691

JOHN B. COSGRAVE

WITH AN INTRODUCTION BY TIM ROBINSON

A prime number with  
2000 digit (40-by-50)

from John Cosgrave, Math Dept,  
St. Patrick's College,  
Dublin, IRELAND.

<http://www.spd.dcu.ie/johnbcos/>

# Primality Testing

Input: A positive integer  $M$ ,  $2^{n-1} < M < 2^n$

**Decision Problem:** Is  $M$  a composite number ?

Decision problem is in NP (guess & verify).

**Search Problem:** Find prime factors of  $M$ .

Factoring integers deterministically is believed to be computationally infeasible.

# Primality Testing

**Question:** Is there a better way to solve the decision problem (test if  $M$  is composite) than by solving the search problem (factoring  $M$ )?

**Basic Idea [Solovay-Strassen, 1977]:**

To show that  $M$  is composite, enough to find **evidence** that  $M$  does **not** behave like a **prime**. Such evidence need not include any prime factor of  $M$ .

# Primality Testing

Evidence that  $M$  is **non prime** may come from Fermat's little theorem:

Any  $1 < a < M$  satisfying  $a^{M-1} \neq 1$  supplies concrete evidence that  $M$  is non prime (**but no factorization!**)

Example:

```
> M:=788888880997:  
> 769967665 &^ (M-1) mod M;  
10621956220
```

$M$  is composite

Will "Fermat test" **always** find such evidence ?

# Primality Testing

There are some  $M$  where Fermat test fails !

Example:

```
> M:= 225593397919:
> 769967665 &^ (M-1) mod M;
      1
> 3222223664 &^ (M-1) mod M;
      1
```

Well, maybe  $M$  is prime after all ?

```
> gcd(6619,M) ;
      6619
```

End of story regarding  $M$ ...

# Carmichael Numbers

Composites  $M$  where Fermat test fails  
( $a^{M-1} = 1$ ) for most  $a$ ,  $1 < a < M-1$ .

Theorem:  $M$  is a Carmichael number iff  
 $M = p_1 p_2 p_3 \dots p_k$  ( $k > 2$ ), all  $p_i$  are distinct primes,  
and every  $p_i$  satisfies  $p_i - 1$  divides  $M - 1$ .

```
Example > M:= 225593397919:    ifactor(M);  
          (15443) (6619) (2207)  
> (M-1) mod 15442 ; (M-1) mod 6618; (M-1) mod 2206;  
          0  
          0  
          0
```

Carmichael numbers: Rare, still infinitely many.

# Evidence that $M$ is non prime

An integer  $a$ ,  $1 < a < M$  such that either

1.  $\gcd(a, M) > 1$  (non trivial factor).
2.  $a^{M-1} \neq 1 \pmod{M}$  (Fermat test).
3.  $a^2 = 1 \pmod{M}$  but  $a \neq M - 1$  ???????

Such integer  $a$  will be called a witness for  $M$  being composite.

# Evidence that $M$ is non prime

A witness  $a$ ,  $1 < a < M$  such that either

1.  $\gcd(a, M) > 1$  implies  $M$  has non trivial factors .
2.  $a^{M-1} \neq 1 \pmod{M}$  implies the size of the multiplicative group  $Z_M^*$  is smaller than  $M-1$ .
3.  $a^2 = 1 \pmod{M}$  but  $a \neq M - 1$  implies 1 has more than two square roots in  $Z_M^*$ .

Back to our favorite  $M=225593397919$

Being a Carmichael number, we won't easily find a witness that is either a non trivial factor or flunks the Fermat test.

Denote  $M-1=2r$ . So  $b^{M-1} = (b^r)^2 = 1 \pmod M$ .

If  $b^r \neq M - 1 \pmod M$ , then  $a=b^r$  is a witness of type (3).

**Gotcha!**

In both cases

$a^2 = 1$  but  $a \neq M - 1$ .

```
> 769967665 &^ ((M-1)/2) mod M;  
187977462064  
> 3222223664 &^ ((M-1)/2) mod M;  
206734298217
```

## Pushing this Idea Further (General $M$ )

Let  $M-1=2^k r$  where  $r$  is odd.

Then  $b^{M-1} = (\dots((b^r)^2)\dots)^2$  ( $k$  squaring ops).

If  $b^{M-1} \neq 1 \pmod M$ , we're all set. Otherwise,

let  $a_0 = b^r$ ,  $a_1 = (a_0)^2$ ,  $a_2 = (a_1)^2$ , ...,  $a_k = (a_{k-1})^2$ .

Then  $a_k = b^{M-1} = 1 \pmod M$ .

Let  $j$  be the smallest index with  $a_j = 1 \pmod M$ .

If  $0 < j$  and  $a_{j-1} \neq M-1$  then  $M$  is composite.

# Evidence that $M$ is Composite

Let  $M-1=2^k r$  where  $r$  is odd.

Pick  $1 < b < M$ .

Compute mod  $M$

$$a_0 = b^r, a_1 = (a_0)^2, a_2 = (a_1)^2, \dots, a_k = (a_{k-1})^2.$$

1. If  $a_k \neq 1$  then  $M$  is composite.

Let  $j$  be the smallest index with  $a_j = 1 \pmod{M}$ .

2. If  $0 < j$  and  $a_{j-1} \neq M-1$  then  $M$  is composite.

Call  $b$  satisfying (1) or (2) a smart witness.

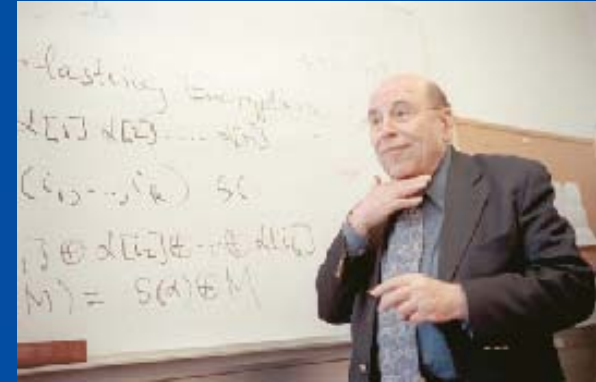
# Miller Theorem (1977)

Let  $M=2^k r+1$  where  $r$  is odd.  
If  $M$  is composite then there  
is\* a small smart witness  $b$   
(small means  $b < (\log M)^2$ ).

\* Assuming a (yet) unproven number theoretic statement: The extended Riemann hypothesis



# Rabin Theorem (1980)



Let  $M=2^k r+1$  where  $r$  is odd.

If  $M$  is composite then at least

$3M/4$  of all  $b$  in the range

$1 < b < M$  are smart witnesses.

No assumption required, and proof employs only elementary tools.

# Miller-Rabin Primality Testing

Input: Odd integer  $M$  ( $2^{n-1} < M < 2^n$ ).

Repeat 100 times:

Pick  $b$  at random ( $1 < b < M$ ).

Check if  $b$  is a smart witness (poly( $n$ ) time).

If one or more  $b$  is a smart witness, output

" $M$  is composite".

Otherwise output " $M$  is prime".

# Miller-Rabin Primality Testing

Properties of Algorithm:

- **Randomized** (uses coin flips to pick **b**'s).
- Run time - polynomial in  $n = \log M$ .
- If **M** is **prime** the algorithm always outputs "**M** is prime".
- If **M** is composite the algorithm may err. However to err, all choices of **b** should give non-witnesses, so  
Probability of error  $< (0.25)^{100} \lll 1$ .

# Primality Testing

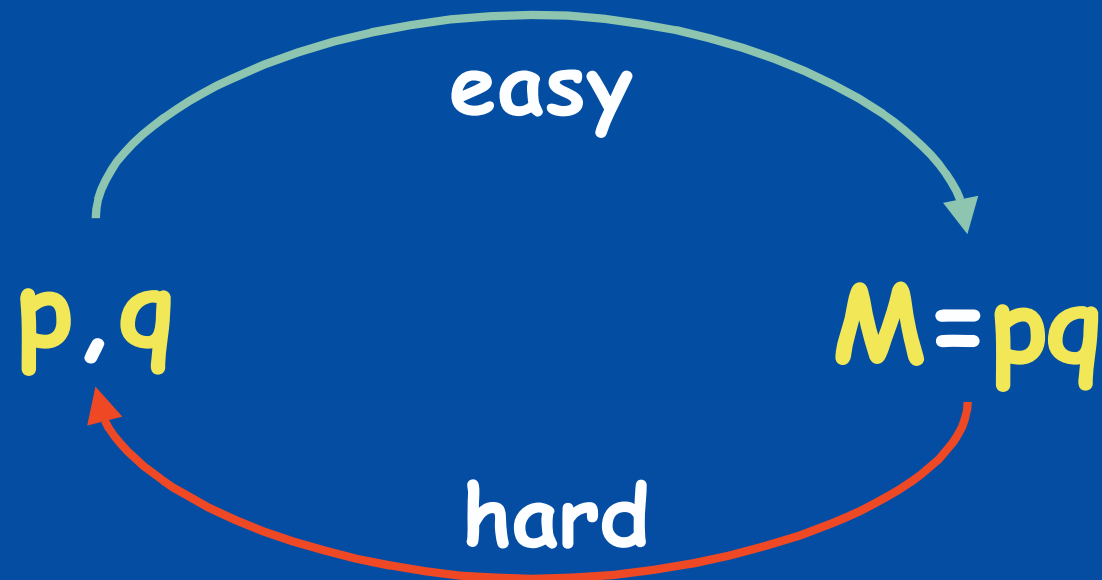
In terms of complexity classes, this algorithm (and its predecessor, Solovay-Strassen algorithm) imply

Composites  $\in$  RP

RP=Random Poly Time, one sided error.

Easy fact: RP is contained in NP.

# Integer Multiplication & Factoring as a One Way Function.



Q.: Can a public key system be based  
on this observation ??????

# Next Lecture (2002)

A.: RSA public key cryptosystem



Rivest



Shamir



Adelman