

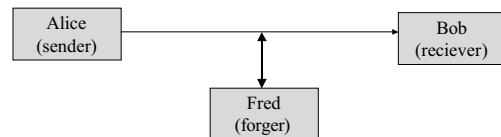
Introduction to Modern Cryptography

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.

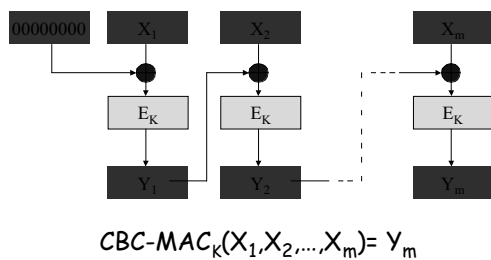
Reminder: MACs

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_K



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)

Primality Testing

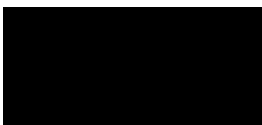
Evidence that M is non prime may come from Fermat's little theorem:
 Any $1 < a < M$ satisfying $a^{M-1} \neq 1$ supplies concrete evidence that M is non prime (but no factorization !)

Example:  M is composite

Will "Fermat test" always find such evidence ?

Primality Testing

There are some M where Fermat test fails !

Example: 

Well, maybe M is prime after all ?

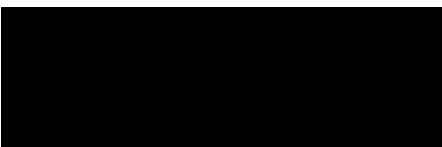


End of story regarding M ...

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: 

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 $a \neq M-1$.

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 $a_0 = b^r$, $a_1 = (a_0)^2$, $a_2 = (a_1)^2, \dots, a_k = (a_{k-1})^2$.
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 $< (0.25)^{100} \lll 1$.

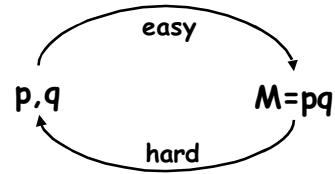
Primality Testing

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