CRYPTOLOGY SOLVES IT ALL?

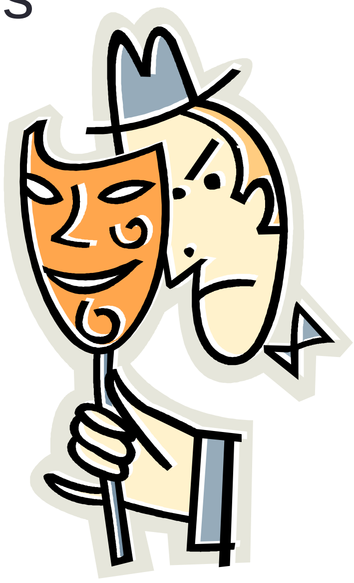
MTH 440

So is that it? Have we solved all the confidentiality problems?

- Alice and Bob want to communicate secretly online
- Use a public key system (e.g. RSA, Diffie-Hellman key exchange) to exchange a private key to be used for a symmetric key algorithm
- Use the exchanged key to encipher communications quickly using the symmetric key algorithm
- Safe from Eve the eavesdropper – even if she hears all communications she can’t figure anything out!
- Fast and efficient!

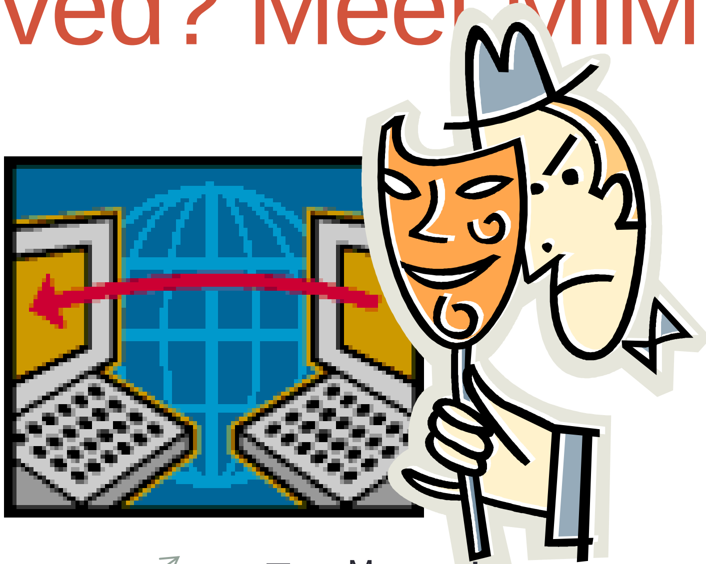
But wait…meet MIM

- MIM is the “man or madam” in the middle.
- Unlike Eve who just eavesdrops MIM actively tries to disrupt or overtake the interactions
- Observe…

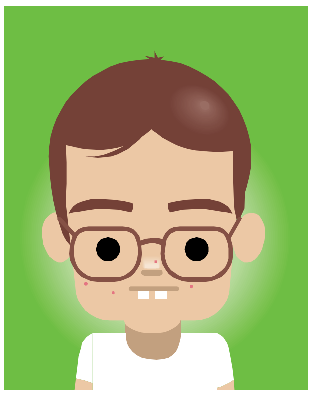


Problem Solved? Meet MIM

Alice



Bob



$Z=g^M \bmod p$

MIM Knows K1 & K2

1. Exchange Key (with MIM)

$g^A \bmod p = Y$

$X = g^B \bmod p$

$K1=g^{AM} \bmod p$

$K2=g^{BM} \bmod p$

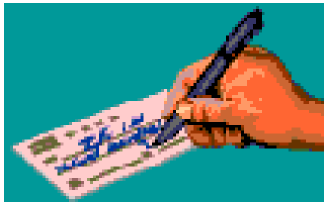
2. Encrypt messages with key K1&K2 – MIM can control it all! Alice and Bob have no idea ☹

What is missing?

- Source Authentication

Digital Signatures

- Like a handwritten signature, an electronic signature is meant to associate data with a person in a verifiable way
- A *cryptographic digital signature* is a cryptographic method for doing that:
  - *Uniquely associates a message with the signer*
  - *Different signatures for different messages*



Example: We can use RSA in a slightly different way.

- Suppose I am “5” (mod 323 of course)
- I send you:
  - Message: 21 (you may or may not care if the message is secret)
  - Signature: 72 (aka “5”)

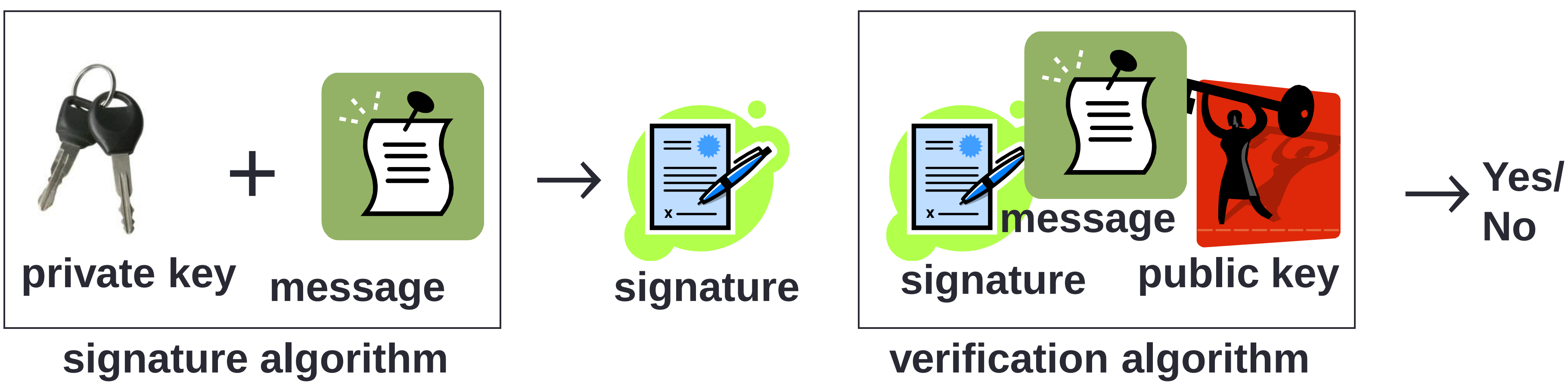
- Is it really from me? Is it from “5”?
- Check – what is 72^5 mod 323?
- Is it 21? If so then I must be “5” (mod 323 of course)
- I used my public key “5” to find a corresponding private key which I use to compute my signature (72) on the message 21. (Each message from 5 will have a different signature). Only someone who can factor 323 can figure this out.

Example: I am “5” (mod 323 of course)

- I send you:
  - Message: 67
  - Signature: 33 (aka “5”)
- Is it really from me? Is it from “5”?
- Check – what is 33^5 mod 323?
- If it is 67, then it must have come from “5”!

Public Key Digital Signatures

- Requires two algorithms and two keys:
  - **The signature algorithm** takes as input a message and the first key, called the secret or *private key* and outputs the signature
  - **The verification algorithm** takes as input the message, signature and the second key, called the *public key* and outputs yes or no.



Public Key Digital Signatures

- The private and public keys are mathematically related, but knowledge of the public key does not allow you to compute the private key
- Hence, if the verification algorithm outputs "yes" using a particular public key, then only the holder of the corresponding private key could have produced the signature

The Mathematics of Digital Signatures

- The first publicly available signature algorithm was created in 1978 by **R**ivest, **S**hamir and **A**dleman and is called RSA
- The security (difficulty of finding the private key given the public key) is based on the hard mathematical problem of factoring large numbers:
  - Sound familiar?

The RSA Digital Signature Scheme

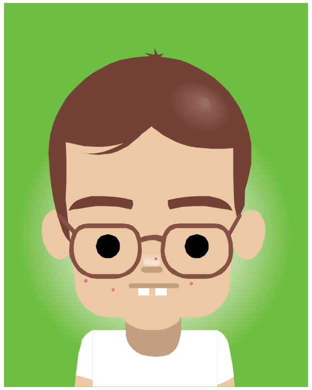
- Let N=pq be the product of two very LARGE prime numbers (p and q are kept secret)
- Choose a secret key d with $0<d<N$
- The public key is (N,e) where $0<e<N$ such that

$$d*e = 1 \bmod \Phi(N)$$

- As we know, given N and e, it is computationally infeasible to find d without knowledge of either $\Phi(N)$ or p and q (which are all secret)

Instead of using N,e to encipher a message to Bob, we use it to check that the signature he gave to us is valid (sort of the reverse of what we have been doing)

RSA Digital Signature



Bob publishes his public key
(N,e)

<u>Verification</u>
To verify the message is from Bob, Alice uses Bob’s public key and checks if

$$M \stackrel{?}{=} Sig(M)^e = M^{de} \bmod N$$

<u>Signature</u>
To sign a message, M, Bob uses his secret key to compute

$$Sig(M) = M^d \bmod N$$

If her check produces M, Alice knows the message was sent from Bob since only he knows d and therefore could have produced such a Sig(M)

Example: Bob's public key: N=15,e=3

Message, Signature

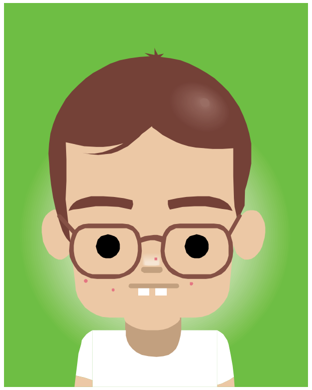
2, 2^{11} = 2048=8 (15) : (2,Sig(2) =8) $\rightarrow$

3, 3^{11} = 12 (15): (3,Sig(3)=12) $\rightarrow$

Verification

8^3=512 = 2 (15)   YES

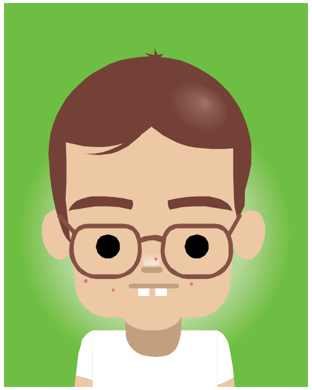
12^3 = 3 (15)   YES



Sign your message – problem solved?

Alice

Bob



1. Exchange Key with signature

$g^A \bmod p = Y$

(X,Sig(Bob,X)) $X = g^B \bmod p$

(Y,sig(Alice,Y))

$K=g^{AB} \bmod p$

$K=g^{AB} \bmod p$

2. Verify signatures are correct

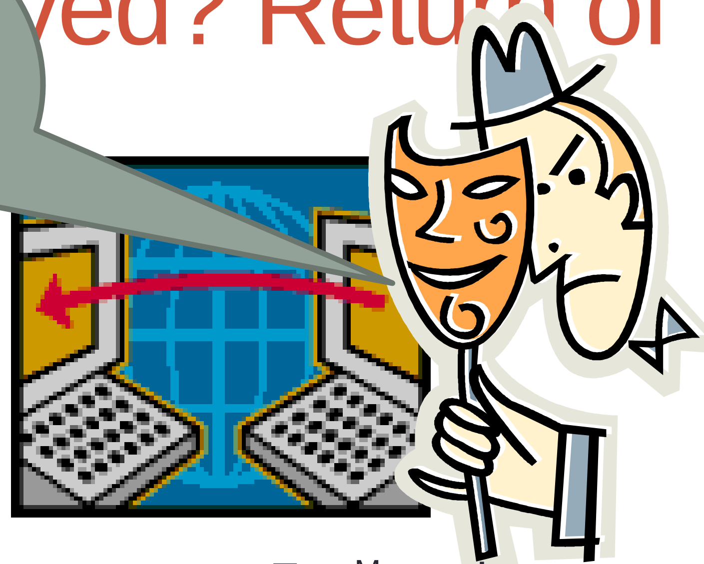
3. Encrypt Messages with Key K

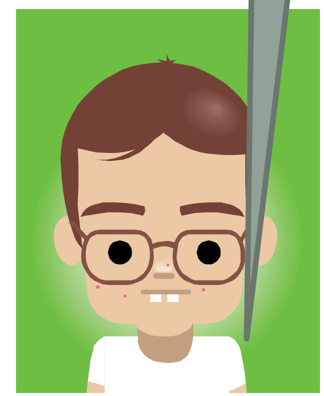
Drat! Those mathematicians have done it again!

ved? Return of MIM

Hey this isn't from Alice!!

Bob





$Z=g^{M} \bmod p$

(Y,sig(Alice,Y))

$g^{A} \bmod p = Y$

(Z,attempted forge on a signature from Alice)

$K1=g^{AM} \bmod p$

In practice

- If the message M is long, then it would take a long time to generate a digital signature on M using RSA.
- In practice first a “message digest” of M is computed using what is called a “hash function”. This creates a fixed length output H(M) that is usually about 160 bits or more, then H(M) is signed.

DSA: The Digital Signature Algorithm

- security based on the discrete logarithm problem
- See handout