Guest Lecture

CSE 100

Professor Martin Tompa from the Computer Science and Engineering Department tells us about ...

FIT 100

Today's topic

Secret Codes,

Unforgeable Signatures,

and

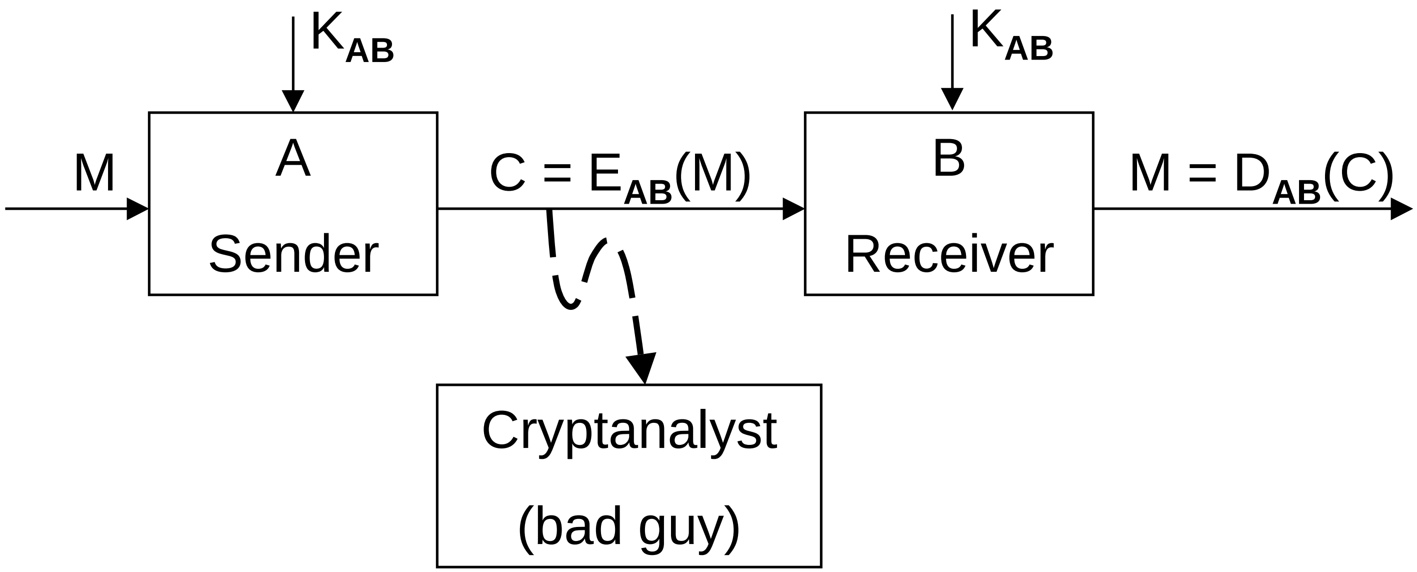
Coin Flipping on the Phone

FIT 100 A Secret Code

John J & Barbara G				
5815 Ann Arbor NE	SEATTLE	98105	206	524-3371
John R Dr 8001 Sand Point Way NE	SEATTLE	98115	206	523-8877
GATELY H A 3847 Woodlawn N	SEATTLE	98103	206	634-2368
Joe & Kelley 15114 SE 224th	KENT	98042	253	639-8073
Kimberlie 5815 Ann Arbor NE	SEATTLE	98105	206	524-0179
Steve & Christina 31500 1st Ave S	FEDWY	98003	253	946-4303
GATENS Clay M			206	352-1590
James 2008 SW 348th	FEDWY	98023	253	838-3565
GATERS M 11300 3d NE	SEATTLE	98125	206	363-1482
GATES A 721 17th	SEATTLE	98122	206	323-3705
A & C Shoreline			206	542-4366
Abraham 820 NE 57th	SEATTLE	98105	206	729-1580
Andrew R 14405 SE 15th	BLVU	98007	425	957-7398
Barron			206	901-1947
Bertha 3014 NE 98th	SEATTLE	98115	206	729-0714

FIT 100

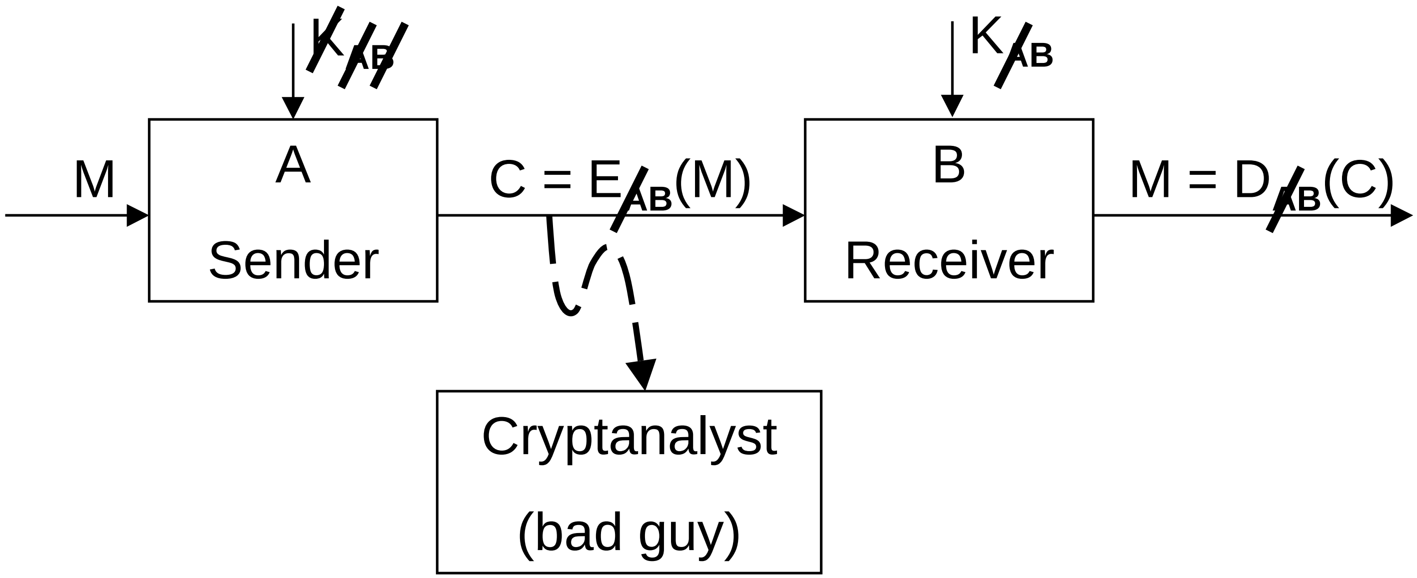
What Is a Cryptosystem?



M	C	K_{AB}
Message	Encryption	Key
Plaintext	Cyphertext	
Cleartext		

FIT 100

What Is a Public Key Cryptosystem?



M	C	K_B	E_B
Message	Encryption	Key	Public Key
Plaintext	Cyphertext	Private Key	
Cleartext			

FIT 100

The RSA Public Key Cryptosystem

- Invented by Rivest, Shamir, and Adleman in 1977.
- Has proven resilient to all cryptanalytic attacks since.

FIT 100

Receiver's Set-Up

- Choose 500-digit primes p and q (each 2 more than a multiple of 3).

  $p = 5$, $q = 11$

- Let $n = pq$.

  $n = 55$

- Let $s = (1/3)\ (2(p - 1)(q - 1) + 1)$.

  $s = (1/3)\ (2 \cdot 4 \cdot 10 + 1) = 27$

- Publish n.

  Keep p, q and s secret.

FIT 100

Encrypting a Message

- Break the message into chunks.

  H I   C H R I S …

- Translate each chunk into an integer M ($0 < M < n$).

  8 9   3 8 18 9 19 …

- Divide M^3 by n. $E(M)$ is the remainder.

  $M = 8$, $n = 55$

  $8^3 = 512 = 9 \times 55 + 17$

  $E(8) = 17$

FIT 100 Decrypting A Cyphertext C

- Divide C^s by n. $D(C)$ is the remainder.

  $C = 17$, $n = 55$, $s = 27$

  $17^{27} = 1{,}667{,}711{,}322{,}168{,}688{,}287{,}513{,}535{,}727{,}415{,}473$

  $= 30{,}322{,}024{,}039{,}430{,}696{,}136{,}609{,}740{,}498{,}463 \times 55 + 8$

  $D(17) = 8$

- Translate $D(C)$ into letters.

  H

FIT 100 Why does it work?

Euler's Theorem (1736): Suppose

- p and q are distinct primes,
- $n = pq,$
- $0 \leq M < n,$ and
- $k > 0.$

If $M^{k(p-1)(q-1)+1}$ is divided by n, the remainder is M.

$$(M^3)^s = (M^3)^{(1/3)(2(p-1)(q-1)+1)}$$

$$= M^{2(p-1)(q-1)+1}$$

FIT 100

Leonhard Euler 1707-1783

FIT 100

Why Is It Secure?

- To find *M = D(C),* you seem to need *s.*
- To find s, you seem to need *p* and *q.*
- All you have is *n = pq.*
- How hard is it to factor a 1000-digit number *n*?

  With the grade school method,

  doing 10,000,000 steps per second

  it would take … 10^{485} years.

FIT 100

State of the Art in Factoring

- 1977: Inventors encrypt a challenge using “RSA129,” a 129-digit number $n = pq$.
- 1981: Pomerance invents a new factoring method.
- 1994: RSA129 factored over an 8 month period using 1000 computers on the Internet around the world.

- With this method, a 250-digit number would take 100,000,000 times as long.

FIT 100

Signed Messages

- How A sends a secret message to B

<u>A</u> <u>B</u>

$C = E_{\boldsymbol{B}}(M)$

C →

$M = D_{\boldsymbol{B}}(C)$

FIT 100

Signed Messages

- How A sends a secret message to B

A		B
$C = E_{\boldsymbol{B}}(M)$		
	C →	
		$M = D_{\boldsymbol{B}}(C)$

- How A sends a signed message to B

A		B
$C = D_{\boldsymbol{A}}(M)$		
	C →	
		$M = E_{\boldsymbol{A}}(C)$

FIT 100 Signed *and* Secret Messages

- How A sends a secret message to B ...

A	B

$C = E_{\boldsymbol{B}}(M)$

C →

$M = D_{\boldsymbol{B}}(C)$

- How A sends a signed secret message to B ...

A	B

$C = E_{\boldsymbol{B}}(D_{\boldsymbol{A}}(M))$

C →

$M = E_{\boldsymbol{A}}(D_{\boldsymbol{B}}(C))$

FIT 100

Flipping a Coin Over the Phone

A		B
Choose random x.		
$y = E_{\mathbf{A}}(x)$		
	y →	
		Guess if x is even or odd.
	← "even" / "odd"	
	x →	
		Check $y = E_{\mathbf{A}}(x)$.

❖ B wins if the guess about x was right