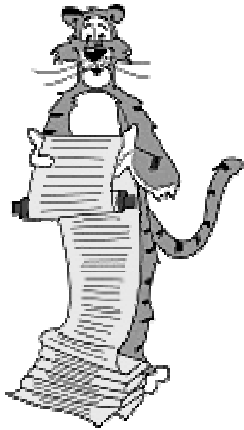


Lecture S1: Cryptology



Cryptology

Cryptology.

- Science of secret communication.



Goal: information security in presence of malicious adversaries.

- Confidentiality.
- Integrity.
- Authentication.
- Authorization.
- Non-repudiation.

Analog Cryptology

Task.

- Protect information.
- Identification.
- Contract.
- Money transfer.
- Public auction.
- Poker.
- Public election.
- Public lottery.
- Anonymous communication.

Analog implementation.

Digital Cryptology

Our goal.

- Implement all tasks digitally.
- Implement additional tasks that can't be done with physics!
 - play poker over phone
 - anonymous elections where everyone learns winner, but nothing else!

Fundamental questions.

- Is any of this possible?
- How?

Today.

- Give flavor of modern digital cryptology.
- Implemented a few of these tasks.
- Sketch a few technical details.

Digital Cryptology Axioms

Axiom 1.

- Players can toss coins.



Axiom 2.

- Players are computationally limited.



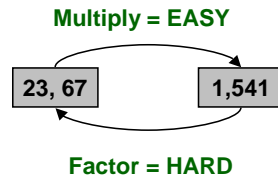
Axiom 3.

- Factoring is hard computationally.



Theorem.

- Digital cryptography exists.



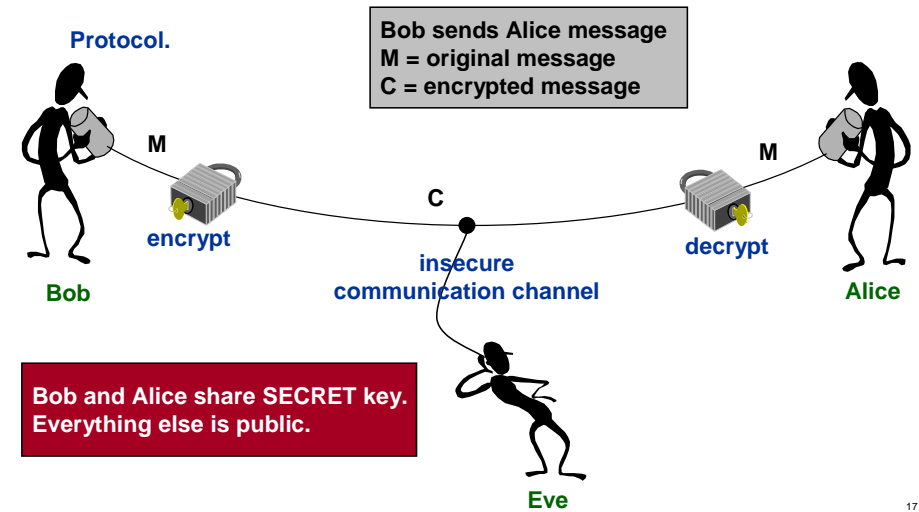
15

Private Key Encryption

Assume message is encoded as binary string.

- ASCII.

Protocol.



17

Private Key Encryption

Bob has N-bit message M to send Alice.

- Alice and Bob share N-bit private key K.
- Bob computes $C = M \wedge K$ and sends C.
- Alice receives C and computes $C \wedge K = (M \wedge K) \wedge K = M$.

\wedge means bitwise XOR

Advantage.



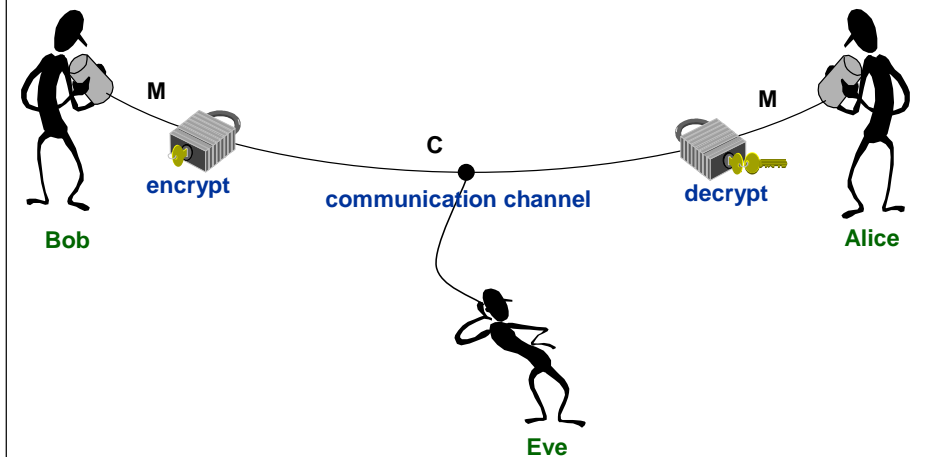
Disadvantage.



0	1	0	1	1	0	M
0	1	1	1	0	0	K
0	0	1	0	1	0	$C = M \wedge K$
0	1	0	1	1	0	$(M \wedge K) \wedge K$

18

Public Key Encryption



20

Public Key Encryption

Bob has N-bit message to send to Alice.

- Alice has public and secret key.
 - PUBLIC key = published on Web in digital phonebook (VeriSign)
 - PRIVATE key = known only by Alice
- Bob encrypts message using Alice's public key.
- Alice decrypts message using her private key.

To achieve security, need following properties:

- Can encrypt message efficiently with public key.
- Can decrypt message efficiently with private key.
- CANNOT decrypt message efficiently with public key alone.

21

Modular Arithmetic

Do all computations modulo some base n.

- $10 + 4 \pmod{12} = 2$
- $38 * 15 \pmod{280} = 570 \pmod{280} = 10$



22

RSA Public-Key Cryptosystem

RSA cryptosystem (Rivest-Shamir-Adleman, 1978).

- Most widely used public-key cryptosystem (500 million users).
- Sun, Microsoft, Apple, browsers, cell phones, ATM machines, . . .

Key generation.

- Select two large prime numbers p and q at random.
- Compute $n = pq$, and $\phi = (p-1)(q-1)$.
- Choose integer e that is relatively prime to ϕ .
- Compute d such that $d e \equiv 1 \pmod{\phi}$.
- Publish (e, n) as public key.
- Keep (d, n) as secret key.

p = 11, q = 29
n = 319, ϕ = 280
e = 3, d = 187
M = 100

Note: don't even need to keep p, q, or ϕ .

- ϕ only needed to compute d.
- Saving p, q speeds up decryption (Chinese Remainder Theorem).

23

RSA Public-Key Cryptosystem

Bob sends message M to Alice.

M < n

- Bob obtains Alice's public key (e, n) from Internet.
- Bob computes $C = M^e \pmod{n}$.

Alice receives message C.

- Alice uses her secret key (d, n).
- Alice computes $M' = C^d \pmod{n}$.

Why does it work? Need $M = M'$. Intuitively.

- $M' \equiv C^d \pmod{n}$
 $\equiv M^{ed} \pmod{n}$
 $\equiv M \quad \text{Recall: } e d \equiv 1 \pmod{\phi}.$
- Argument not rigorous because of mod.
 - rigorous argument uses fact that p and q are prime, and $\phi = (p-1)(q-1)$.

24

RSA Example

Parameters.

- $p = 47, q = 79, n = 3713, \phi = 3588$
 $e = 17, d = 3377$
- $M = 2003$

$$\begin{aligned} & 2003^{17} \pmod{3713} \\ &= 2003^{16} * 2003^1 \pmod{3713} \\ &= 3157 * 2003 \pmod{3713} \\ &= 6323471 \pmod{3713} \\ &= 232 \end{aligned}$$

Modular exponentiation.

- $2003^{17} \pmod{3713}$
 $= 134454746427671370568340195448570911966902998629125654163 \pmod{3713}$
 $= 232$

Better alternative (repeated squaring).

- $2003^1 \pmod{3713} = 2003$
- $2003^2 \pmod{3713} = 4,012,009 \pmod{3713} = 1969$
- $2003^4 \pmod{3713} = 1969^2 \pmod{3713} = 589$
- $2003^8 \pmod{3713} = 589^2 \pmod{3713} = 1612$
- $2003^{16} \pmod{3713} = 3157$

25

RSA Details

How large should $n = pq$ be?

- 1,024 bits for long term security.
- IE, Netscape: 40, 56, 128 bit.
- Too small \Rightarrow easy to break.
- Too large \Rightarrow time consuming to encrypt/decrypt.

How to choose large "random" prime numbers?

- Miller-Rabin procedure checks whether x is prime. Usually!
- Number theory $\Rightarrow n / \log_e n$ prime numbers between 2 and n .

How to compute d efficiently?

- Existence guaranteed since $\gcd(e, \phi) = 1$.
- Fancy version of Euclid's algorithm.

26

RSA Attacks

Factoring.

- Factor $n = pq$.
- Then compute ϕ .
- Then compute e .

Timing attacks.

- Reconstruct d by sending C and monitoring how long it takes to compute $C^d \pmod{n}$.

Other means?

- Long-standing open research question.

Note: Diffie-Helman cryptosystem can be broken if and only if factoring is hard.

- Discrete log: given x, n, C , find d such that $x^d \pmod{n} = C$.

27

Digital Signature

Alice sends Bob a response.

- Bob's wants to be sure Alice really sent it, and not some imposter.



28

RSA Digital Signature

Alice wants to send Bob a response S.

- Alice uses private key d and computes: $S' \equiv S^d \pmod{n}$.
- Alice sends (S, S').

Bob receives digital signed response (S, S').

- Bob uses Alice's public key e and checks if $S \equiv (S')^e \pmod{n}$.
- If yes, then Bob concludes S sent by Alice.
- If no, then Bob concludes S or S' corrupted in transmission, or message is a forgery.

Note: $S^{ed} = S^{de} = S$
(commutativity)

Third party.

- Bob verifies Alice's signature on digitally signed message (e.g., electronic check).
- Bob forwards digitally signed message to bank.
- Bank re-verifies Alice's signature.

29

RSA Tradeoffs

Advantages.



Disadvantages.



30

RSA Applications

Secure Internet communication.

- Browsers.
- S/MIME, SSL, S/WAN.
- PGP.
- Microsoft Outlook.

Operating systems.

- Sun, Microsoft, Apple, Novell.

Hardware.

- Cell phones.
- ATM machines.
- Wireless ethernet cards.
- Smart cards (Mondex).
- Palm Pilots.

31

Bad Cryptology

Content Scrambling System (CSS).

- Used to encrypt DVD's.
- Each disc has 3 40-bit keys.
- Each DVD decoder (software/hardware) has unique 40-bit key.
- "Not possible" to play back on computer without disc.

DeCSS. (Canman and SøupaFrøg, 1999).

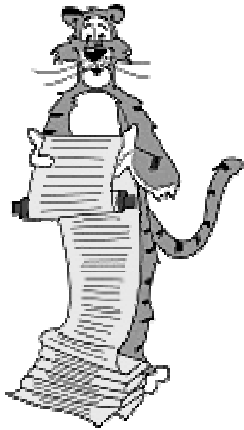
- Decryption algorithm written by two Norwegians
- Used "in-circuit emulator" to monitor hardware activity.

Why CSS is fatally flawed.



32

Cryptography: Extra Slides



RSA Public-Key Cryptosystem

Why does it work? Rigorously.

$$\begin{aligned} M' &= C^d \pmod{n} \\ &= M^{ed} \pmod{n} \end{aligned}$$

Now, since $\phi = (p-1)(q-1)$ and $e d \equiv 1 \pmod{\phi}$

$$ed = 1 + k(p-1)(q-1) \text{ for some integer } k.$$

A little manipulation.

$$\begin{aligned} M^{ed} &\equiv M M^{(p-1)k(q-1)} \pmod{p} \\ &\equiv M (1)^{k(q-1)} \pmod{p} \\ &\equiv M \pmod{p} \end{aligned}$$

(trivially true if $M \equiv 0$)

$$M^{ed} \equiv M \pmod{q}$$

Finally.

$$M^{ed} \equiv M \pmod{\underbrace{pq}_n}$$

Fermat's Little Theorem

if p is prime, then for all $a \neq 0$
 $a^{p-1} \equiv 1 \pmod{p}$

Chinese Remainder Theorem

if p, q prime then for all x, a
 $x \equiv a \pmod{pq} \iff$
 $x \equiv a \pmod{p}, x \equiv a \pmod{q}$