University of Colorado **Boulder**

CSCI 3403 INTRO TO CYBERSECURITY

Lecture: 3-1

Topic: Asymmetric Encyrption

Presenter: Matt Niemiec

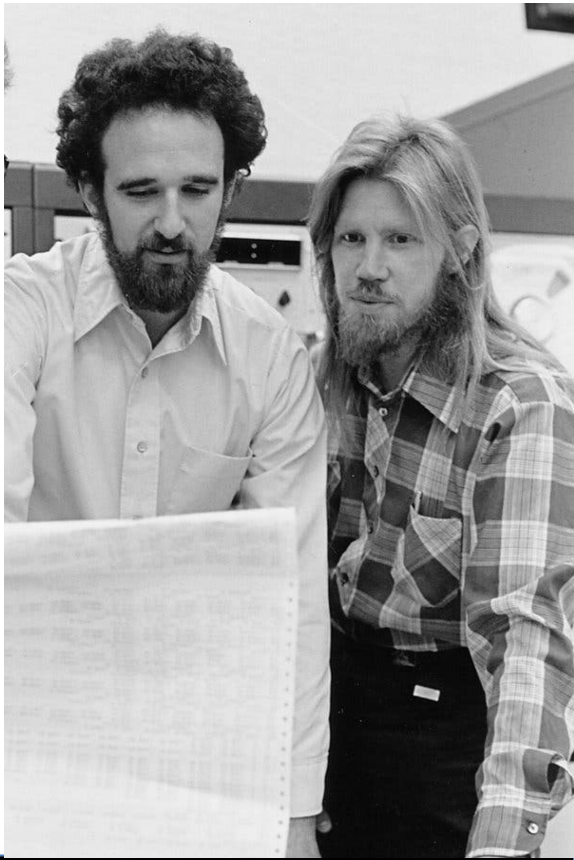
Announcements

- Clarification on extra credit
- Please fill out the groups survey by January 30
- You'll be able to submit project 1 shortly after that
- Don't forget about the survey for any suggestions
  - Link: https://forms.gle/WRUUbPkmFNsa6q3D6
- Survey for Javascript experience

Asymmetric Encryption

One Simple Idea...

- What if the encryption key and decryption key were two different keys? - 1976
  - What if the decryption key could encrypt as well?
  - Completely changed cryptography
- Challenged somebody to find a secure way of doing this



Public Key Visual

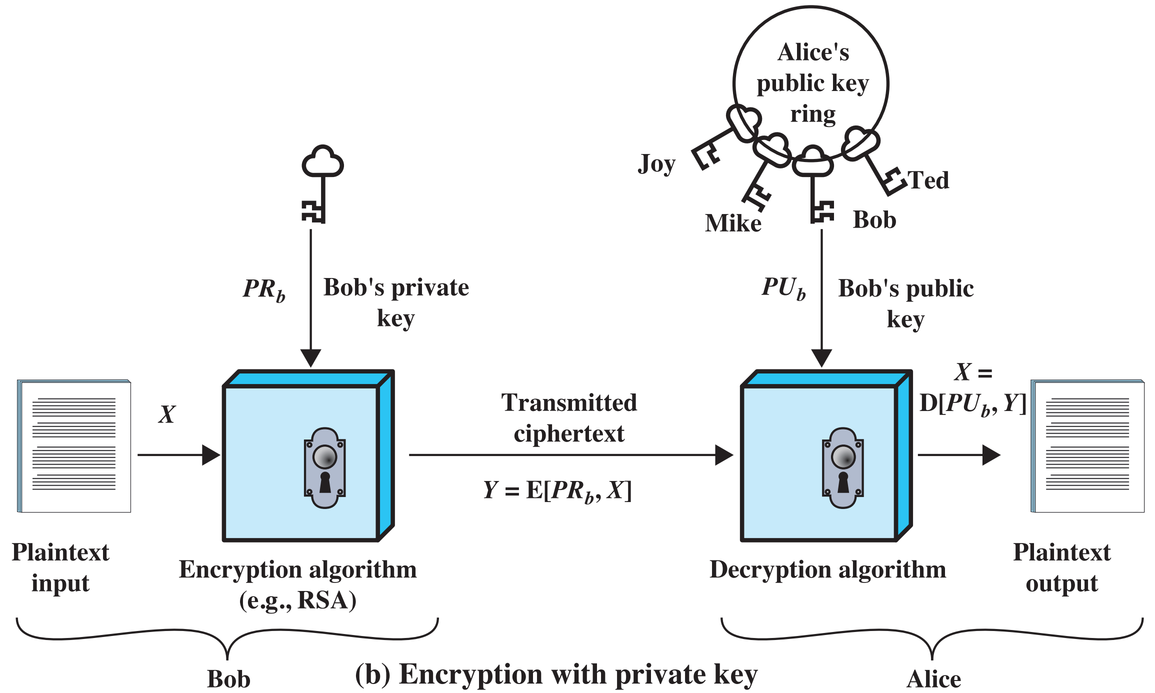
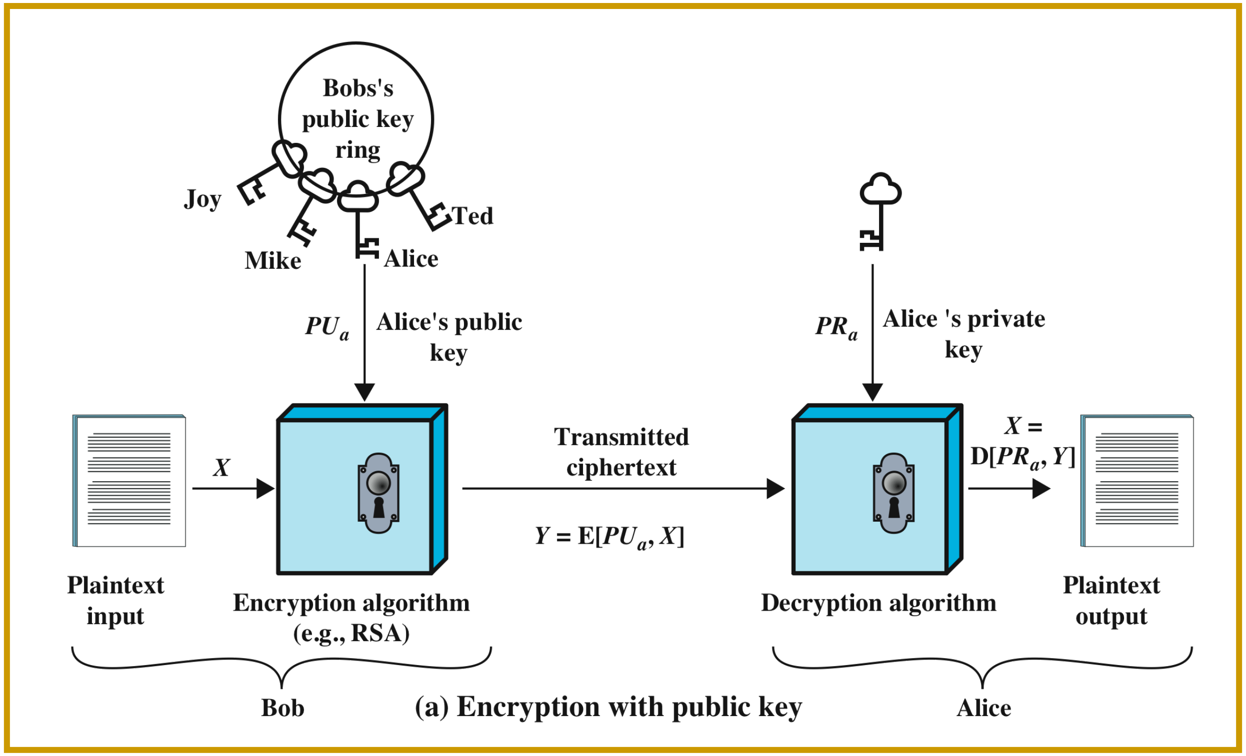


Figure 2.6 Public-Key Cryptography

Public Key Visual



Why?

- Key exchange
- Create message for one person
- Write messages with private key

Diffie-Hellman Key Exchange

- Simple way to exchange keys
- Corrected formula below

1) Generate prime p and base $g<p$
2) Each party picks private value $x <p-1$
3) Each party calculates $y=g^x mod\ p$ and sends it
4) Calculate key $z=y^x mod\ p$

Key Exchange Example

$p = 17$

$g = 12$

Person 1	Person 2
$x = 13$	$x = 4$

Key Exchange Example

$p = 17$

$g = 12$

Person 1

$x = 13$

$y_1 = 12^{13} \bmod 17$

Person 2

$x = 4$

$y_2 = 12^4 \bmod 17$

Key Exchange Example

$p = 17$

$g = 12$

Person 1	Person 2
$x = 13$	$x = 4$
$y_1 = 12^{13} \bmod 17 = 14$	$y_2 = 12^{4} \bmod 17 = 13$

Key Exchange Example

$p = 17$

$g = 12$

Person 1	Person 2
$x = 13$	$x = 4$
$y_1 = 12^{13} \bmod 17 = 14$	$y_2 = 12^4 \bmod 17 = 13$
$z = y_2^x \bmod p$	$z = y_1^x \bmod p$

Key Exchange Example

$p = 17$

$g = 12$

Person 1

$x = 13$

$y_1 = 12^{13} \bmod 17 = 14$

$z = y_2^x \bmod p$

$z = 13^{13} \bmod 17 = ?$

Person 2

$x = 4$

$y_2 = 12^4 \bmod 17 = 13$

$z = y_1^x \bmod p$

$z = 14^4 \bmod 17 = ?$

Key Exchange Example

$p = 17$

$g = 12$

Person 1

$x = 13$

$y_1 = 12^{13} \bmod 17 = 14$

$z = y_2^{x} \bmod p$

$z = 13^{13} \bmod 17 = 13$

Person 2

$x = 4$

$y_2 = 12^{4} \bmod 17 = 13$

$z = y_1^{x} \bmod p$

$z = 14^{4} \bmod 17 = 13$

Diffie-Hellman Key Exchange

- Both parties get the same key
- Somebody listening can’t determine the key
- Problems?

Requirements of Public Key Cryptosystems

Computationally easy to create key pairs

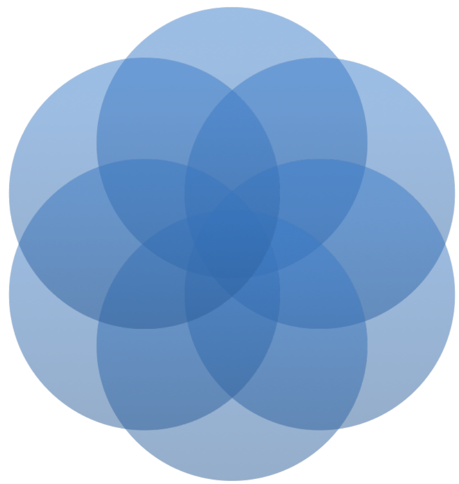
Computationally easy for sender knowing public key to encrypt messages

Computationally easy for receiver knowing private key to decrypt ciphertext

Computationally infeasible for opponent to determine private key from public key

Computationally infeasible for opponent to otherwise recover original message

Useful if either key can be used for each role



RSA

- Rivest, Shamir, and Adleman: “Hold my beer” – 1977
- Most commonly used today

RSA Key Generation Algorithm

1) Select two primes, p and q, $p \neq q$
2) Calculate $n = p \times q$
3) Calculate $\varphi(n) = (p-1)(q-1)$
4) Select e s.t. $GCD(\varphi(n), e) = 1$ and $e < \varphi(n)$
5) Calculate d in $de \bmod \varphi(n) = 1$
6) Your public key is $\{e, n\}$
7) Your private key is $\{d, n\}$

RSA Encryption/Decryption Algorithm

Encryption

1) Plaintext is $M < n$
2) Ciphertext is $C = M^e \bmod n$

Decryption

1) Ciphertext is C
2) Plaintext is $M = C^d \bmod n$

Elliptic Curve Cryptography (ECC)

- Considered as secure as RSA
- Much newer and coming out
  - Smaller key size
  - Not as trusted
- The future of encryption?

Shortcomings of Public Key Crypto

- This seems amazing!
- Is slooooow...
- Relies on unsolved problems in math
- What else?

Solution: Certificate Authority

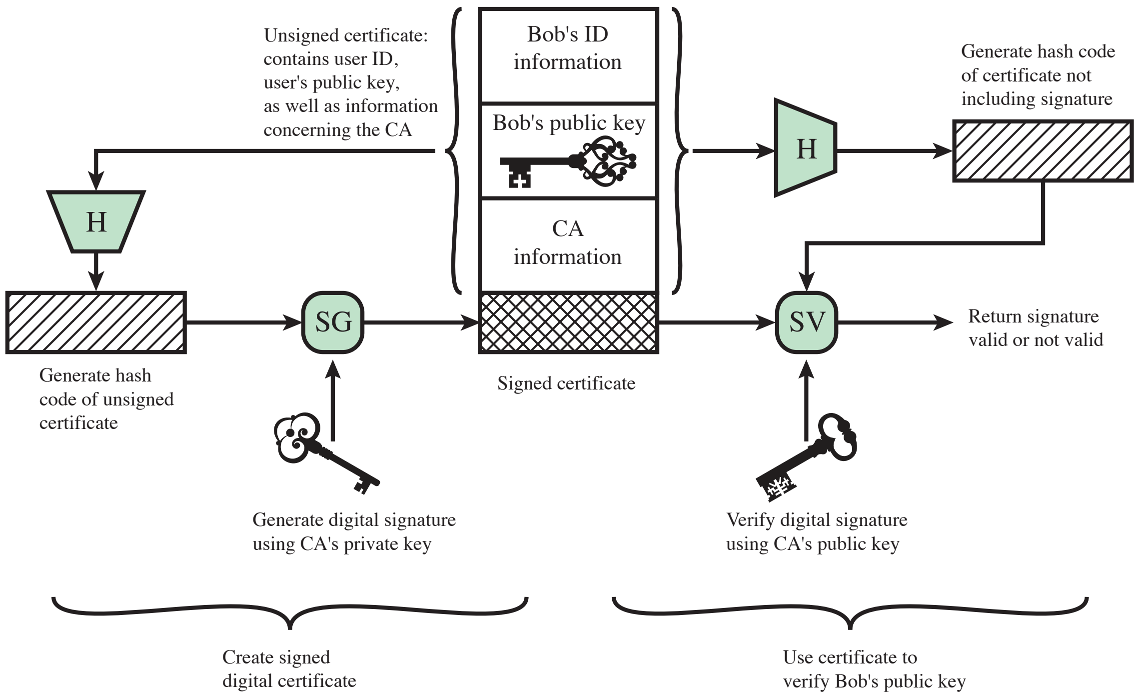


Figure 2.8 Public-Key Certificate Use

Problem With Solution

CRYPTOGRAPHY

Ten Risks of PKI: What You're not Being Told about Public Key Infrastructure

By Carl Ellison and Bruce Schneier

Computer security has been victim of the "year of the..." syndrome. First it was firewalls, then intrusion detection systems, then VPNs, and now certification authorities (CAs) and public-key infrastructure (PKI). "If you only buy X,"

Open any article on PKI in the popular or technical press and you're likely to find the statement that a PKI is desperately needed for e-commerce to flourish. This statement is patently false. E-commerce is already flourish-

Uses of Public Key Crypto

Key Exchange

- Want to communicate over insecure channel
  - Need a way to communicate
- Key encryption vs key distribution

Digital Signatures

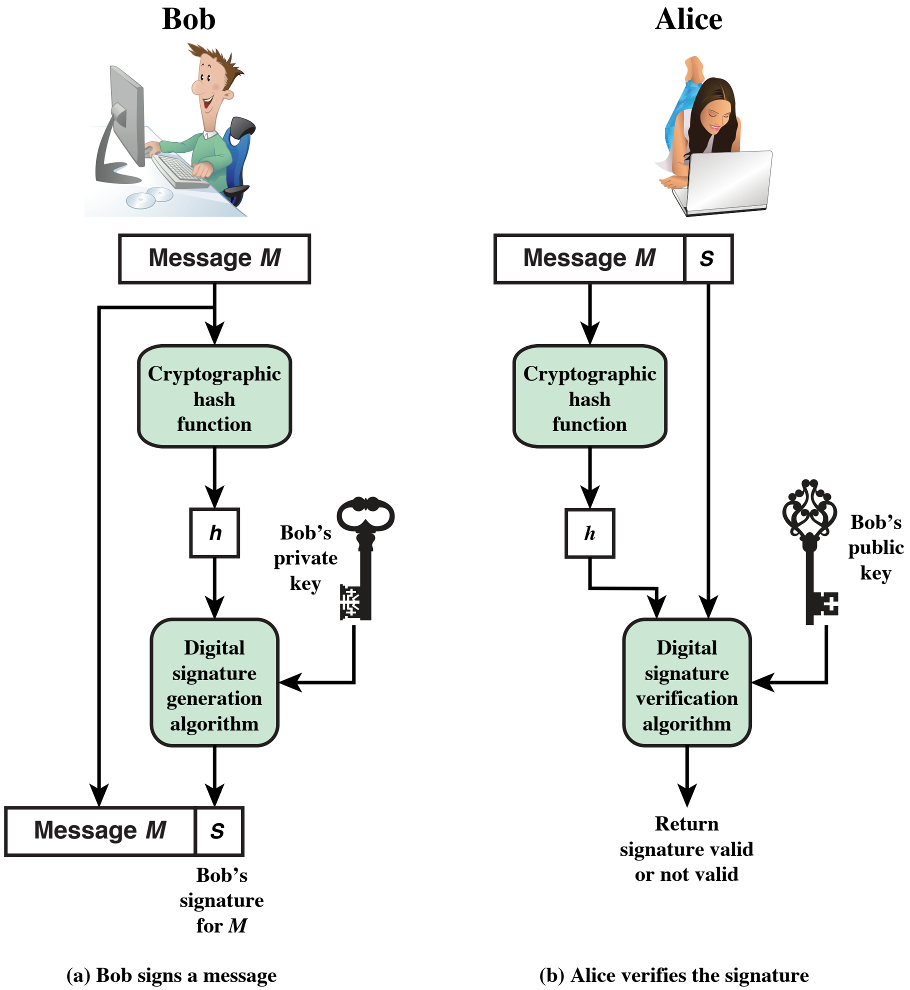


Figure 2.7 Simplified Depiction of Essential Elements of Digital Signature Process

Digital Envelopes

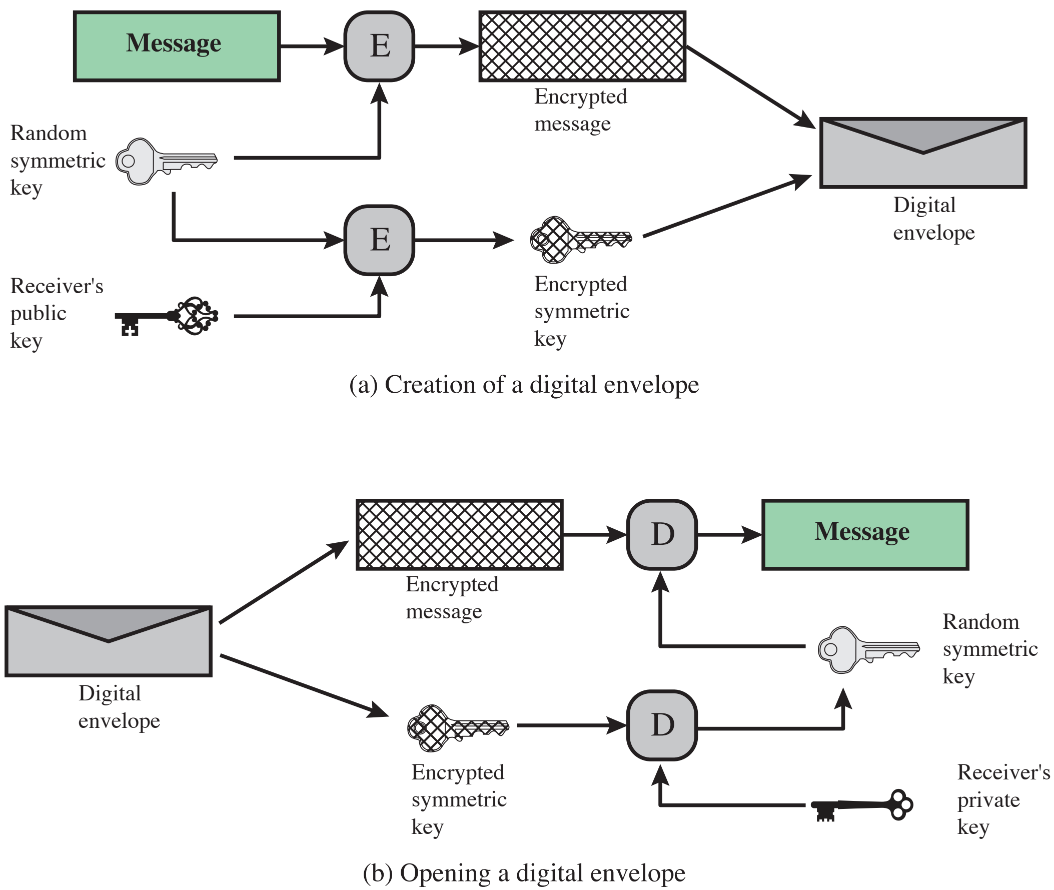


Figure 2.9 Digital Envelopes

Two-Way Communication

- How would we make this work?