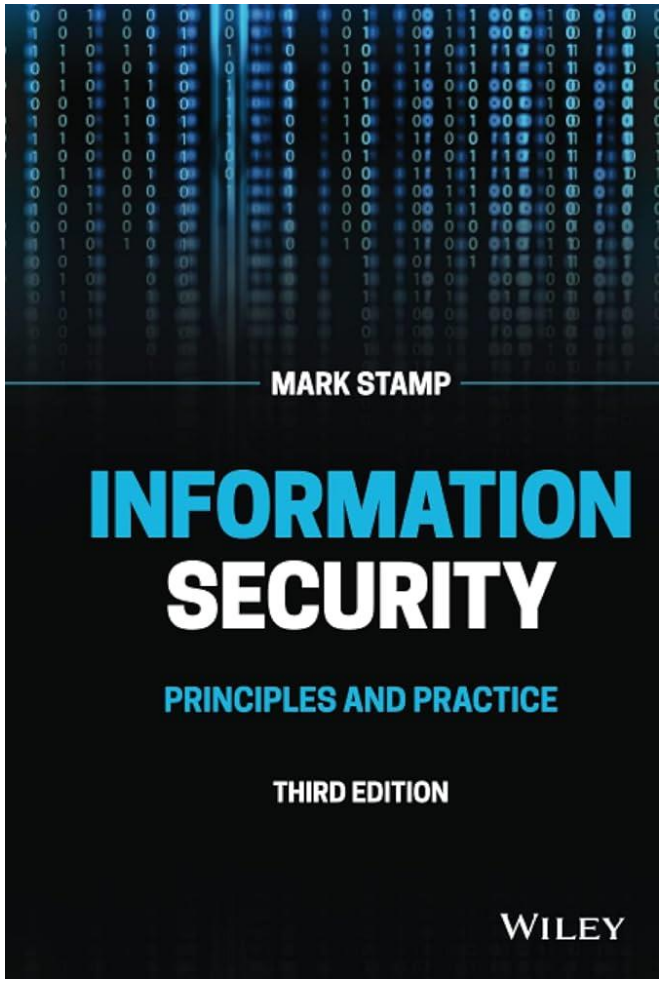
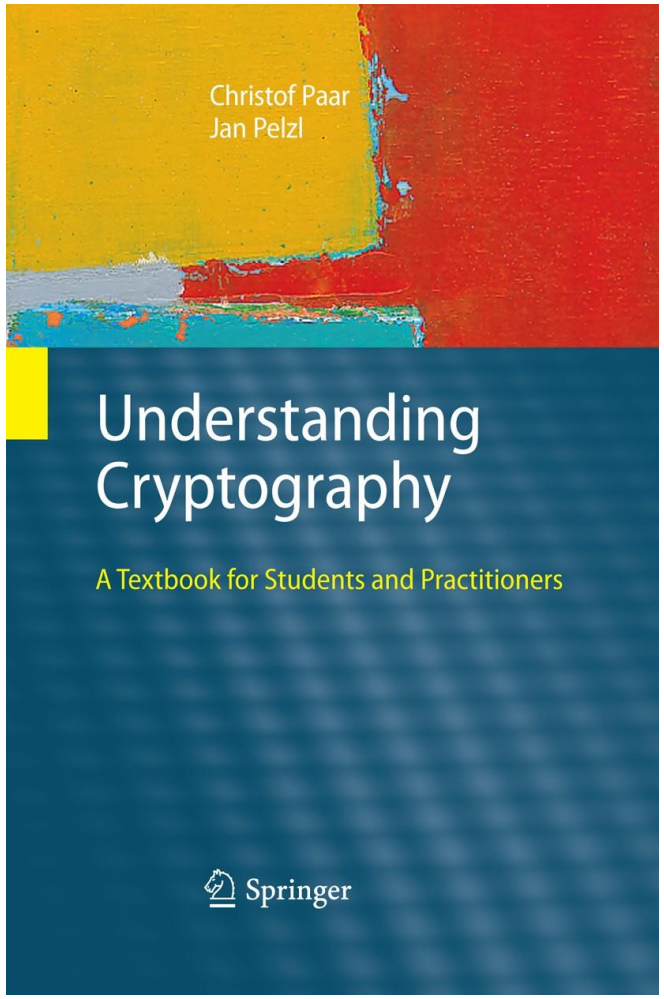
بسم الله الرحمن الرحیم

مبانی رایانش امن

جلسه ۹

مجتبی خلیلی
دانشکده برق و کامپیوتر
دانشگاه صنعتی اصفهان





◀ فصل دهم پار (امضا)

Digital Signature

Basic Digital Signature Protocol

Alice		Bob
		generate $k_{pr,B}$, $k_{pub,B}$
	$\xleftarrow{k_{pub,B}}$	publish public key
		sign message: $s = \text{sig}_{k_{pr}}(x)$
	$\xleftarrow{(x,s)}$	send message + signature
verify signature: $\text{ver}_{k_{pub,B}}(x,s) = \text{true/false}$		

RSA Signature

Basic RSA Digital Signature Protocol

Alice		**Bob**
		$k_{pr} = d,\ k_{pub} = (n, e)$
	$\xleftarrow{(n,e)}$	
		compute signature: $s = \text{sig}_{k_{pr}}(x) \equiv x^d \bmod n$
	$\xleftarrow{(x,s)}$	

verify: $\text{ver}_{k_{pub}}(x, s)$

$x' \equiv s^e \bmod n$

$$x' \begin{cases} \equiv x \bmod n & \Longrightarrow \text{valid signature} \\ \not\equiv x \bmod n & \Longrightarrow \text{invalid signature} \end{cases}$$

Non-non-repudiation

- Alice orders 100 shares of stock from Bob
- Alice computes **MAC** using symmetric key
- Stock drops, Alice claims she did ***not*** order
- Can Bob prove that Alice placed the order?
- **No!** Bob also knows the symmetric key, so he could have forged the **MAC**
- **Problem:** Bob knows Alice placed the order, but he can't prove it

Non-repudiation

- Alice orders 100 shares of stock from Bob
- Alice **signs** order with her private key
- Stock drops, Alice claims she did not order
- Can Bob prove that Alice placed the order?
- **Yes!** Alice's private key used to sign the order — only Alice knows her private key
- This assumes Alice's private key has not been lost/stolen

Elliptic Curve Cryptography

Elliptic Curve Crypto (ECC)

- "Elliptic curve" is **not** a cryptosystem
- Elliptic curves provide different way to do the math in public key system
- Elliptic curve versions of DH, RSA, ...
- Elliptic curves are more efficient
  - Fewer bits needed for same security
  - But the operations are more complex, yet it is a big "win" overall

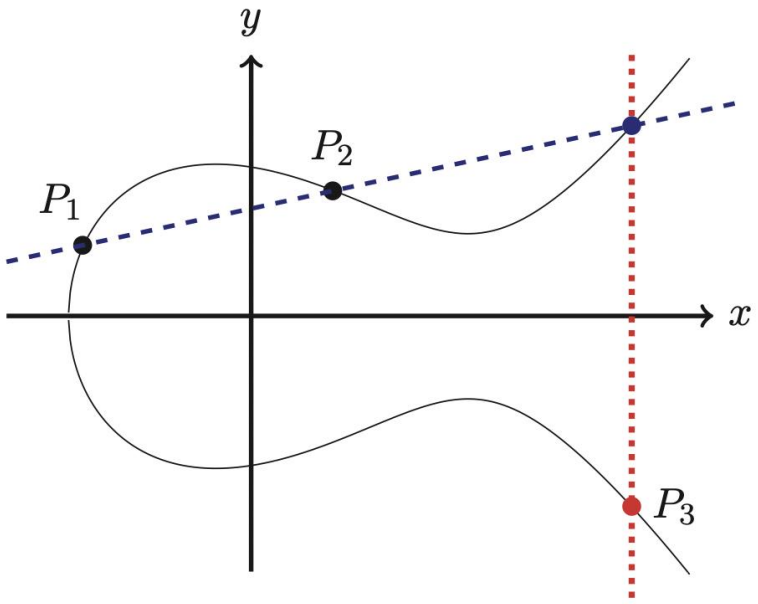
What is an Elliptic Curve?

- An elliptic curve E is the graph of an equation of the form

$$y^2 = x^3 + ax + b$$

- Also includes a "point at infinity"
- What do elliptic curves look like?
- See the next slide!

Elliptic Curve Picture



- Consider elliptic curve

$$E: y^2 = x^3 - x + 1$$

- If P_1 and P_2 are on E, we can define addition,

$$P_3 = P_1 + P_2$$

  as shown in picture
- Addition is all we need…

Uses for Public Key Crypto

- Confidentiality
  - Transmitting data over insecure channel
  - Secure storage on insecure media
- Authentication protocols (later)
- Digital signature
  - Provides integrity and **non-repudiation**
  - No non-repudiation with symmetric keys

Algorithm Family	Cryptosystems	Security Level (bit)			
		80	128	192	256
Integer factorization	RSA	1024 bit	3072 bit	7680 bit	15360 bit
Discrete logarithm	DH, DSA, Elgamal	1024 bit	3072 bit	7680 bit	15360 bit
Elliptic curves	ECDH, ECDSA	160 bit	256 bit	384 bit	512 bit
Symmetric-key	AES, 3DES	80 bit	128 bit	192 bit	256 bit

Public Key Notation

- **Sign** message M with Alice's **private key**: $[M]_{Alice}$
- **Encrypt** message M with Alice's **public key**: $\{M\}_{Alice}$

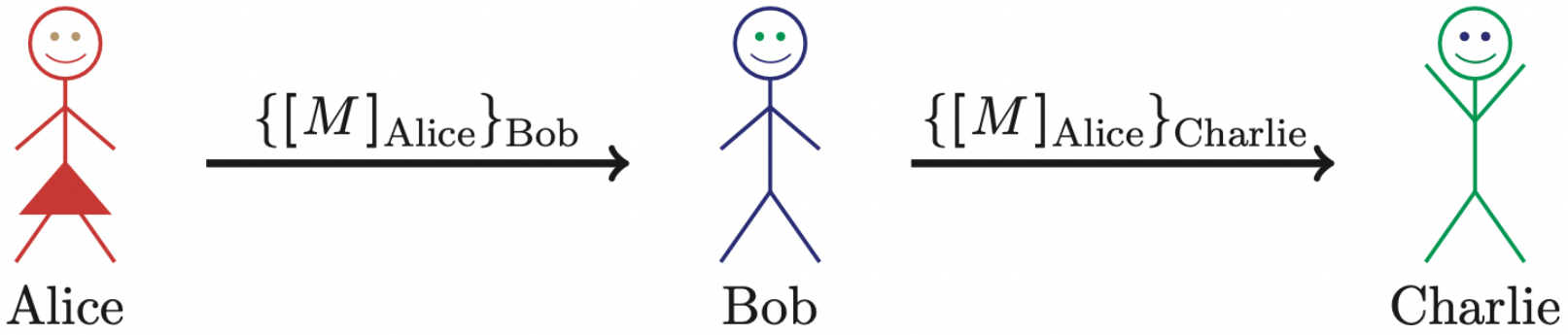
Sign and Encrypt
vs
Encrypt and Sign

Confidentiality and Non-repudiation?

- Suppose that we want confidentiality and integrity/non-repudiation
- Can public key crypto achieve both?
- Alice sends message to Bob
  - **Sign and encrypt:** $\{[M]_{Alice}\}_{Bob}$
  - **Encrypt and sign:** $[\{M\}_{Bob}]_{Alice}$
- Can the order possibly matter?

Sign and Encrypt

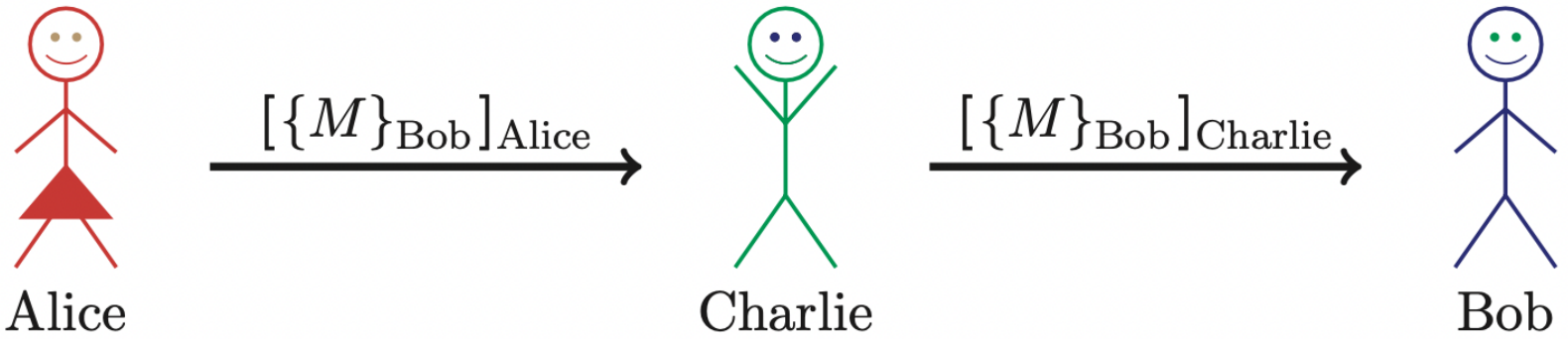
- M = "I love you"



- **Q:** What's the problem?
- ***A*:** No problem — public key is public

Encrypt and Sign

- M = "My theory, which is mine…."



- **Note** that Charlie cannot decrypt M
- **Q:** What is the problem?
- ***A*:** No problem — public key is public

Quantum Computers and Public Key Crypto

- Recall that quantum computing ***not*** a serious threat to symmetric ciphers
- But, QC is a **BIG** threat to public key
- Shor's factoring algorithm (1994)
  - Most famous quantum algorithm
- Let n be number of bits in N, then…
  - Work factor of $n^2 \log_2(n) \log_2(\log_2(n))$

Quantum Computers and Public Key Crypto

- Shor's algorithm much faster than best classic factoring algorithm
  - Number field sieve is best classic alg.
- For a 2048-bit modulus, work factor…
  - Number field sieve equivalent to exhaustive search for 125-bit key
  - Shor's algorithm equivalent to exhaustive search for 30-bit key

Quantum Computers and Public Key Crypto

- Bottom line?
- QC will make RSA obsolete
- Post-quantum cryptography?
  - Symmetric ciphers will be OK
  - Most popular public key algorithms will fail (RSA, Diffie-Hellman, …)
- But there exist public key algorithms that are secure against QC
  - For example, NTRU