



**MSA UNIVERSITY**  
جامعة أكتوبر للعلوم الحديثة والآداب

Established by Dr. Nawal El Deghdy

# Cryptography

## ECE5632 - Spring 2026

### Lecture 8B

**Dr. Farah Raad**

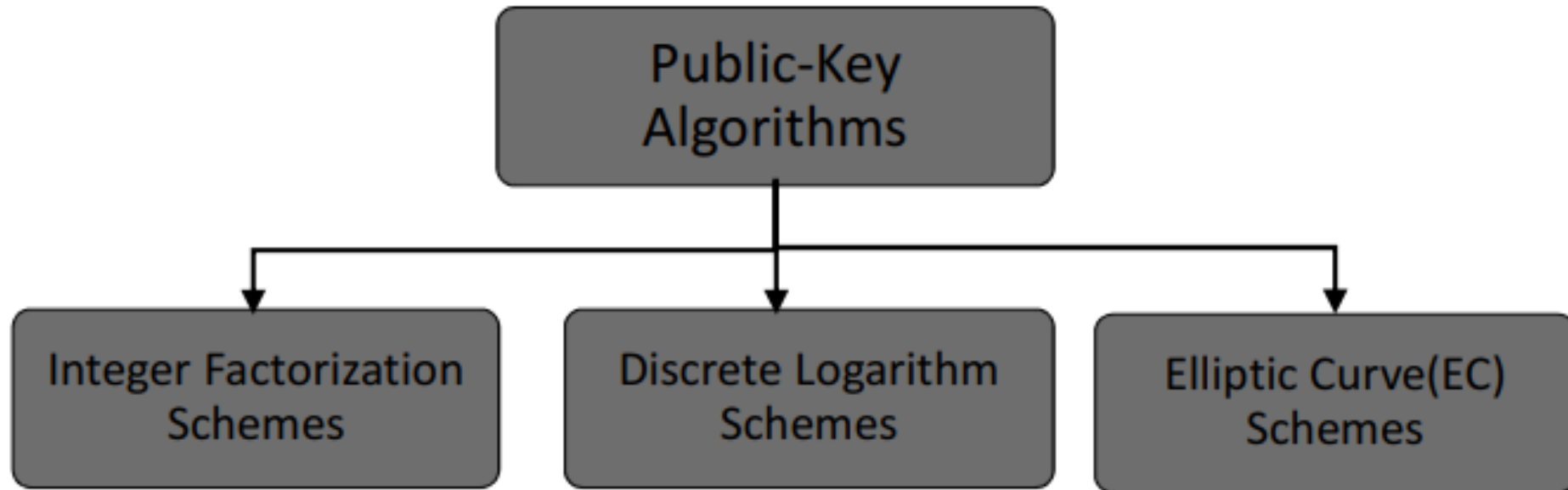
The First British Higher Education in Egypt



# Lecture Topic

# Digital Signature

# PKC Algorithms: Three Families



e.g.

- RSA algorithm.

e.g.:

- Diffie–Hellman key exchange.
- ElGamal encryption.
- Digital Signature Algorithm (DSA).

e.g.:

- EC Diffie–Hellman key exchange (ECDH).
- EC Digital Signature Algorithm (ECDSA).

# Security Services

The objectives of a security systems are called *security services*.

**There are many security services. Most importantly:**

- **Confidentiality:** Information is kept secret from all but the authorized parties.
- **Message Authentication:** The sender of a message is authentic.
- **Message Integrity:** Message has not been modified during transmission.
- **Nonrepudiation:** The sender of a message can't deny the creation of the message.



# Intro to Digital Signature

So far we assumed two honest people and an attacker in between.



We securely share a secret key and encrypt data in between.

But, what if ...



Our goal: Verify the authenticity of a sender.

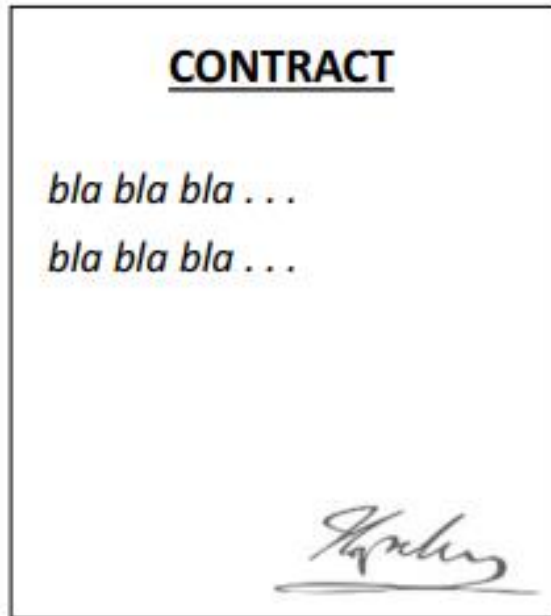
# Intro to Digital Signature

- Alice orders a pink car from the car salesman Bob
- After seeing the pink car, Alice states that she has never ordered it:
- How can Bob prove towards a judge that Alice has ordered a pink car? (And that he did not fabricate the order himself)
  - ❑ Symmetric cryptography fails because both Alice and Bob can be malicious
  - ❑ Can be achieved with public-key cryptography



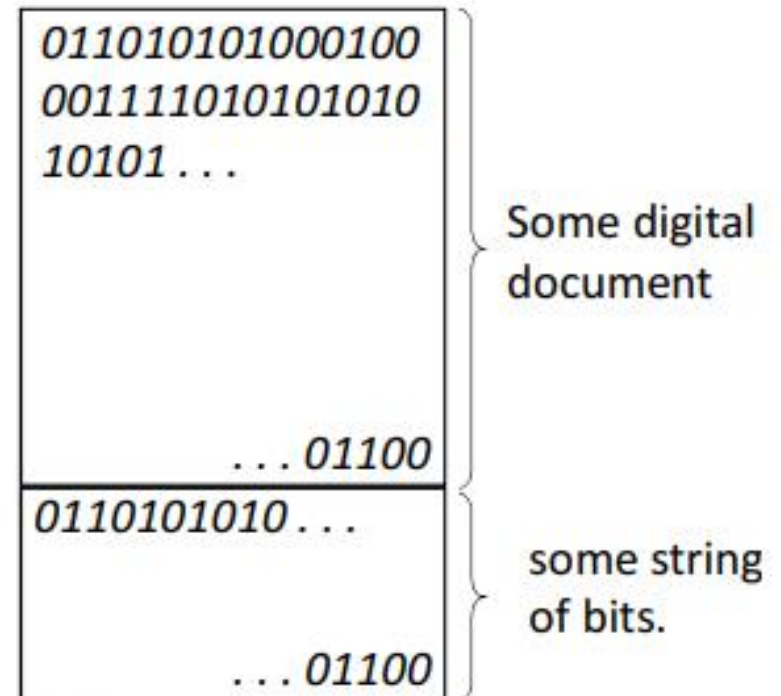
# Intro to Digital Signature

Conventionally, handwritten signatures are used to verify authenticity.



The unique signature is simply added to the document.  
It works.

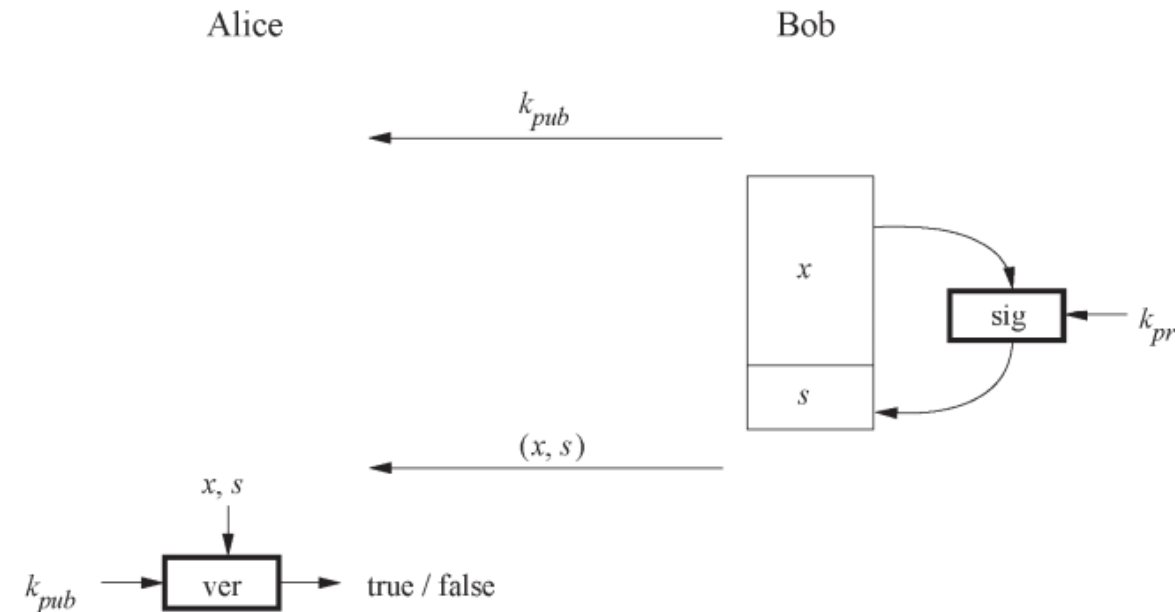
Digitally, things are a bit different.



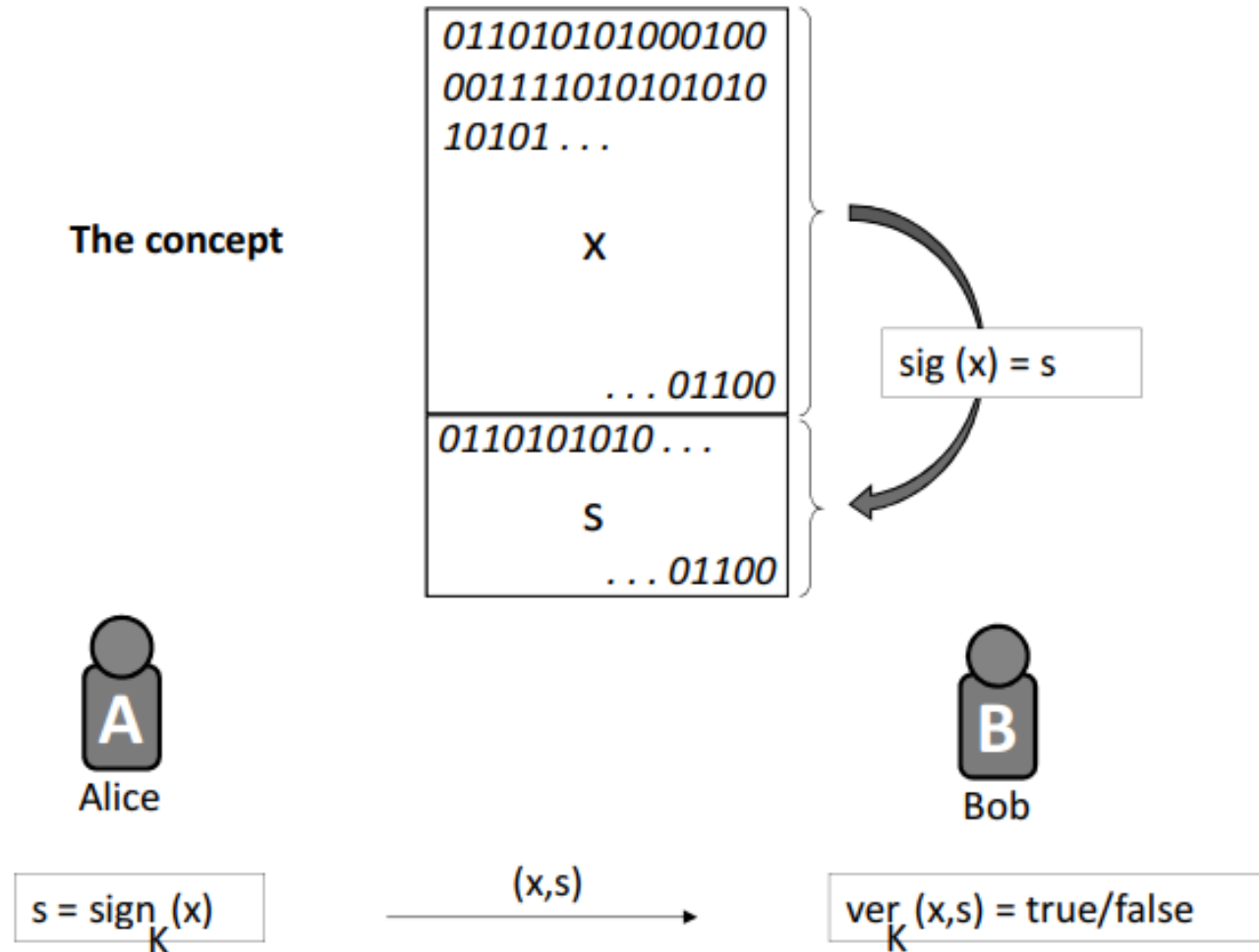
Unlike handwritten signatures, this can be easily faked.

# Basic Concept of Digital Signatures

- For a given message  $x$ , a digital signature is appended to the message (just like a conventional signature).
  - Only the person with the private key should be able to generate the signature.
  - The signature must change for every document.
- ⇒ The signature is realized as a function with the message  $x$  and the private key as input.
- ⇒ The public key and the message  $x$  are the inputs to the verification function.



# Basic Concept of Digital Signatures



Alice can deny signing the message if the signing key is shared.

# RSA Digital Signature

## To generate the private and public key:

- Use the same key generation as RSA encryption.

## To generate the signature:

- “encrypt” the message  $x$  with the private key

$$s = \text{sig}_{K_{\text{priv}}}(x) = x^d \text{ mod } n$$

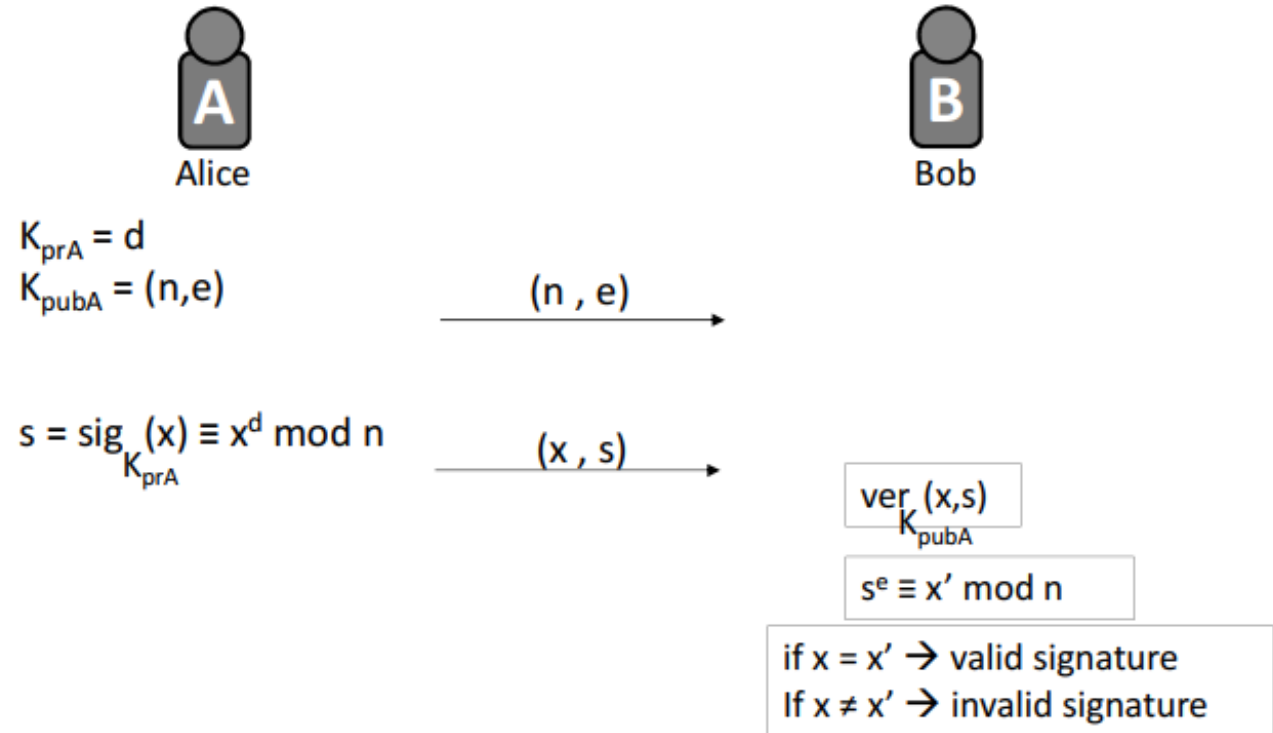
- Append  $s$  to message  $x$

## To verify the signature:

- “decrypt” the signature with the public key

$$x' = \text{ver}_{K_{\text{pub}}}(s) = s^e \text{ mod } n$$

If  $x=x'$ , the signature is valid



# RSA Digital Signature: Example

Suppose Bob wants to send a signed message ( $x = 4$ ) to Alice using RSA signature. Given  $p = 3$  and  $q = 11$ . Compute signature as the sender and verify it as the receiver.

**Alice**

**Bob**

1. choose  $p = 3$  and  $q = 11$
2.  $n = p \cdot q = 33$
3.  $\Phi(n) = (3 - 1)(11 - 1) = 20$
4. choose  $e = 3$
5.  $d \equiv e^{-1} \equiv 7 \pmod{20}$

$(n,e)=(33,3)$



compute signature for message

$x = 4$ :

$$s = x^d \equiv 4^7 \equiv 16 \pmod{33}$$

$(x,s)=(4,16)$



verify:

$$x' = s^e \equiv 16^3 \equiv 4 \pmod{33}$$

$$x' \equiv x \pmod{33} \implies \text{valid signature}$$



# ElGamal Digital Signature

## Key Generation for Elgamal Digital Signature

1. Choose a large prime  $p$ .
2. Choose a primitive element  $\alpha$  of  $\mathbb{Z}_p^*$  or a subgroup of  $\mathbb{Z}_p^*$ .
3. Choose a random integer  $d \in \{2, 3, \dots, p-2\}$ .
4. Compute  $\beta = \alpha^d \bmod p$ .

The public key is now formed by  $k_{pub} = (p, \alpha, \beta)$ , and the private key by  $k_{pr} = d$ .

## Elgamal Signature Generation

1. Choose a random ephemeral key  $k_E \in \{0, 1, 2, \dots, p-2\}$  such that  $\gcd(k_E, p-1) = 1$ .
2. Compute the signature parameters:

$$r \equiv \alpha^{k_E} \bmod p,$$
$$s \equiv (x - d \cdot r) k_E^{-1} \bmod p-1.$$



# ElGamal Digital Signature

## Elgamal Signature Verification

1. Compute the value

$$t \equiv \beta^r \cdot r^s \pmod{p}$$

2. The verification follows from:

$$t \begin{cases} \equiv \alpha^x \pmod{p} & \implies \text{valid signature} \\ \not\equiv \alpha^x \pmod{p} & \implies \text{invalid signature} \end{cases}$$



# ElGamal Digital Signature



Alice



Bob

Choose prime  $p$

Choose primitive element  $\alpha$

$$k_{pr} = d \in \{2, \dots, p-2\}$$

$$k_{pub} = \beta \equiv \alpha^d \pmod{p}$$

ephemeral key  $k_E \in \{2, \dots, p-2\}$ ,  
such that  $\gcd(k_E, p-1) = 1$

$$r \equiv \alpha^{k_E} \pmod{p}$$

$$s \equiv (x - d \cdot r) K_E^{-1} \pmod{p-1}$$

$(\beta, p, \alpha)$



$x, (r, s)$



Verify

$$t \equiv \beta^r r^s \pmod{p}$$

If  $t \equiv \alpha^x \pmod{p} \rightarrow$  valid sign

If  $t \not\equiv \alpha^x \pmod{p} \rightarrow$  invalid sign

# ElGamal Digital Signature

Proof of correctness:

$$\begin{aligned}\beta^r r^s &\equiv (\alpha^d)^r (\alpha^{K_E})^s \pmod{p} \\ &\equiv \alpha^{d.r + K_E.s} \pmod{p} \equiv \alpha^x \pmod{p}\end{aligned}$$

$$\text{Let } a^m = a^{q(p-1)+r} = (a^q)^{p-1} a^r$$

From Fermat's Little Theorem,

$$(a^q)^{p-1} \equiv 1 \pmod{p}$$

$$a^m \pmod{p} \equiv a^r \pmod{p}$$

$$\text{Then } \mathbf{a^m \pmod{p} \equiv a^{m \pmod{p-1}} \pmod{p}}$$

$$\text{So, } d.r + K_E.s \equiv x \pmod{p-1}$$

$$s \equiv (x - d.r) K_E^{-1} \pmod{p-1}$$

# ElGamal Digital Signature: Example

Bob wants to send a message to Alice. This time, it should be signed with the Elgamal digital signature scheme.

**Alice**

**Bob**

1. choose  $p = 29$
2. choose  $\alpha = 2$
3. choose  $d = 12$
4.  $\beta = \alpha^d \equiv 7 \pmod{29}$

$(p, \alpha, \beta) = (29, 2, 7)$

compute signature for message  
 $x = 26$ :

choose  $k_E = 5$ , note that  
 $\gcd(5, 28) = 1$

$$r = \alpha^{k_E} \equiv 2^5 \equiv 3 \pmod{29}$$

$$s = (x - dr)k_E^{-1} \equiv (-10) \cdot 17 \equiv 26 \pmod{28}$$

$(x, (r, s)) = (26, (3, 26))$

verify:

$$t = \beta^r \cdot r^s \equiv 7^3 \cdot 3^{26} \equiv 22 \pmod{29}$$

$$\alpha^x \equiv 2^{26} \equiv 22 \pmod{29}$$

$$t \equiv \alpha^x \pmod{29} \implies \text{valid signature}$$





# Thank You!

**See You next Lectures!!**  
**Any Question?**

**THE FIRST BRITISH HIGHER EDUCATION IN EGYPT**

26th July Mehwar Road Intersection with Wahat Road, 6th of October City, Egypt

**Tel:** +202383711146 **Fax:** +20238371543 **Postal code:** 12451

**Email:** [info@msa.eun.eg](mailto:info@msa.eun.eg) **Hotline:** 16672 **Website:** [www.msa.edu.eg](http://www.msa.edu.eg)