Cryptography
ECE5632 - Spring 2024

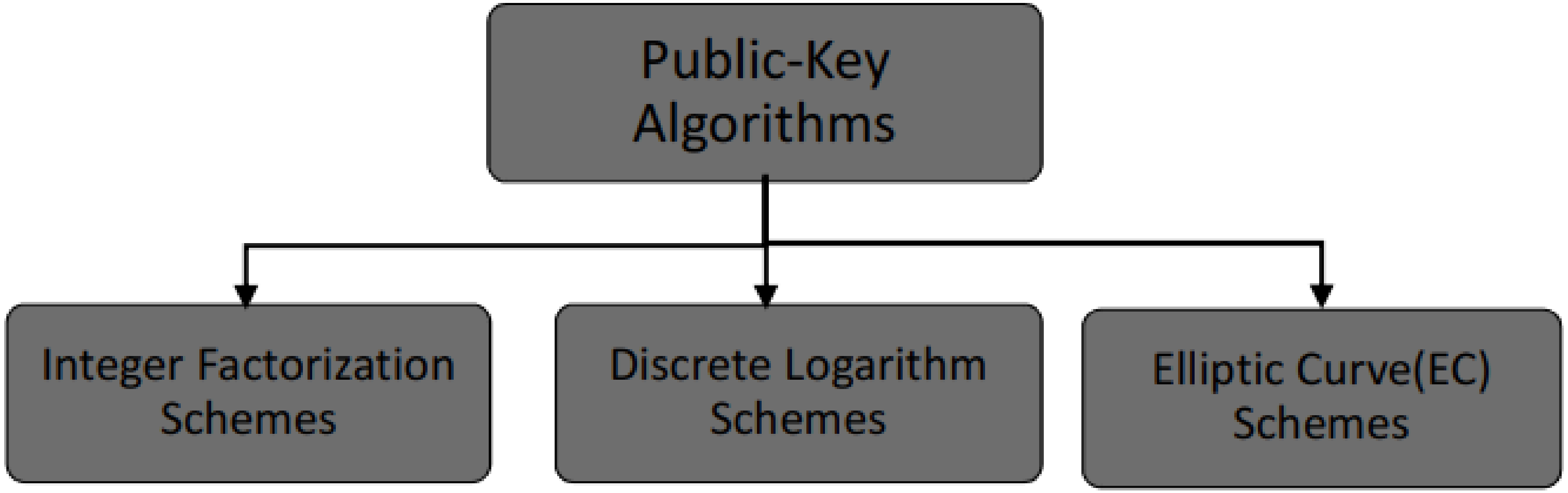
Lecture 8B

Dr. Farah Raad

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.

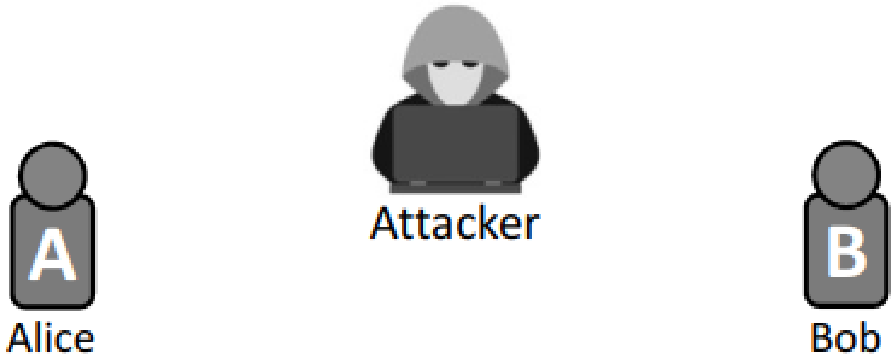
- **Message Authentication:** The sender of a message is authentic.

- **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 ...

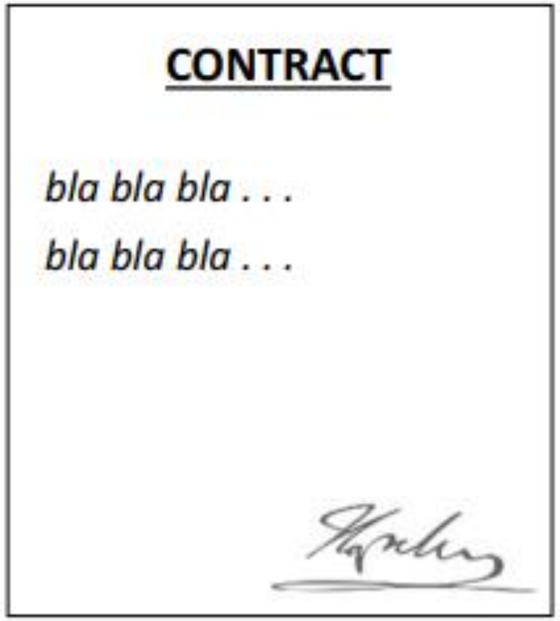
Our goal: Verify the authenticity of a sender.

Intro to Digital Signature

- Alice orders a pink car from the car salesmen 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

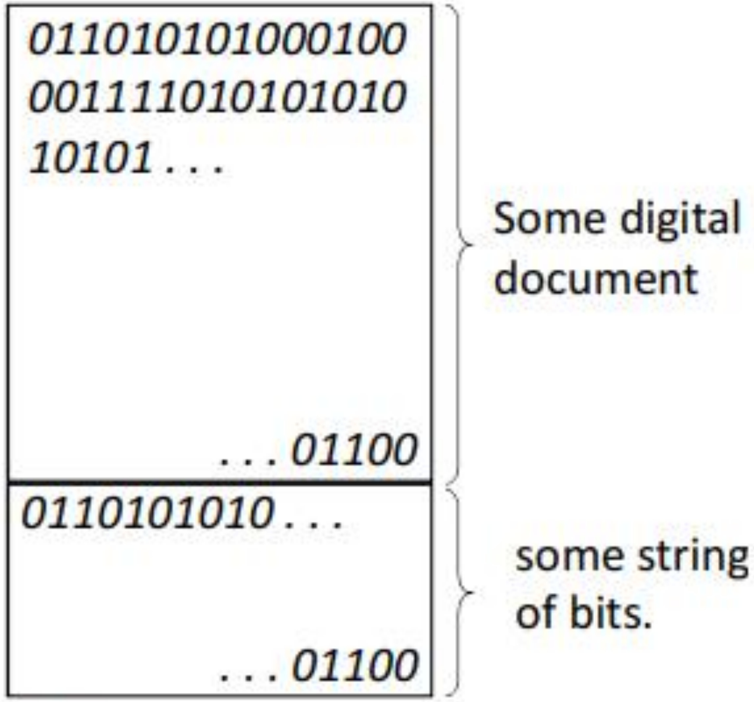
Intro to Digital Signature

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.



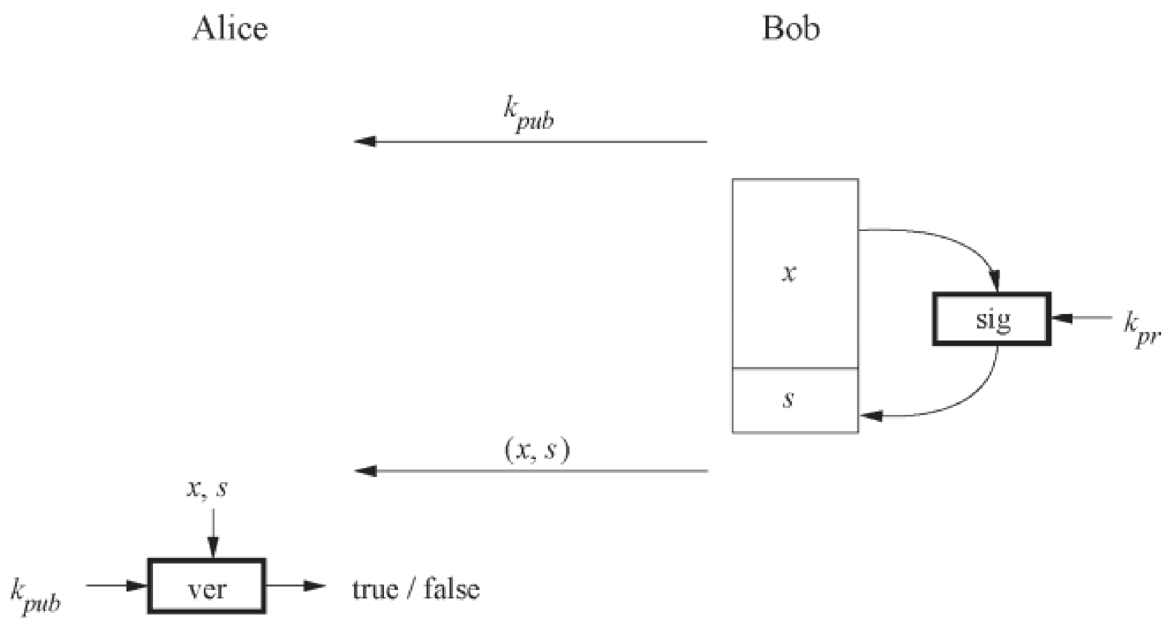
Unlike handwritten signatures, this can be easily faked.

Basic Concept of Digital Signatures

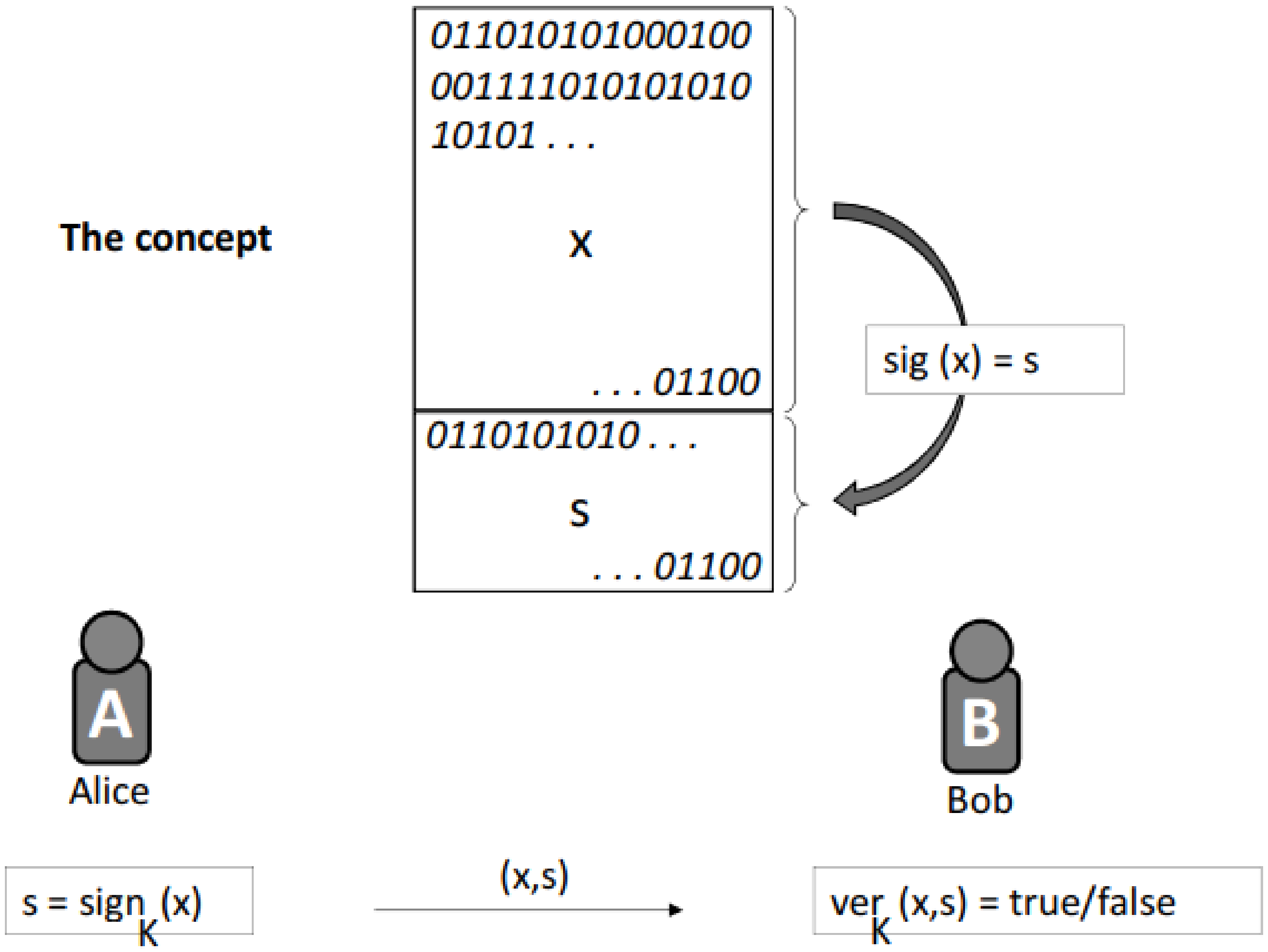
- For a given message x, a digital signature is appended to the message (just like a conventional signature).

- 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

$$\boxed{s = sig_{K_{priv}}(x) = x^d \bmod n}$$

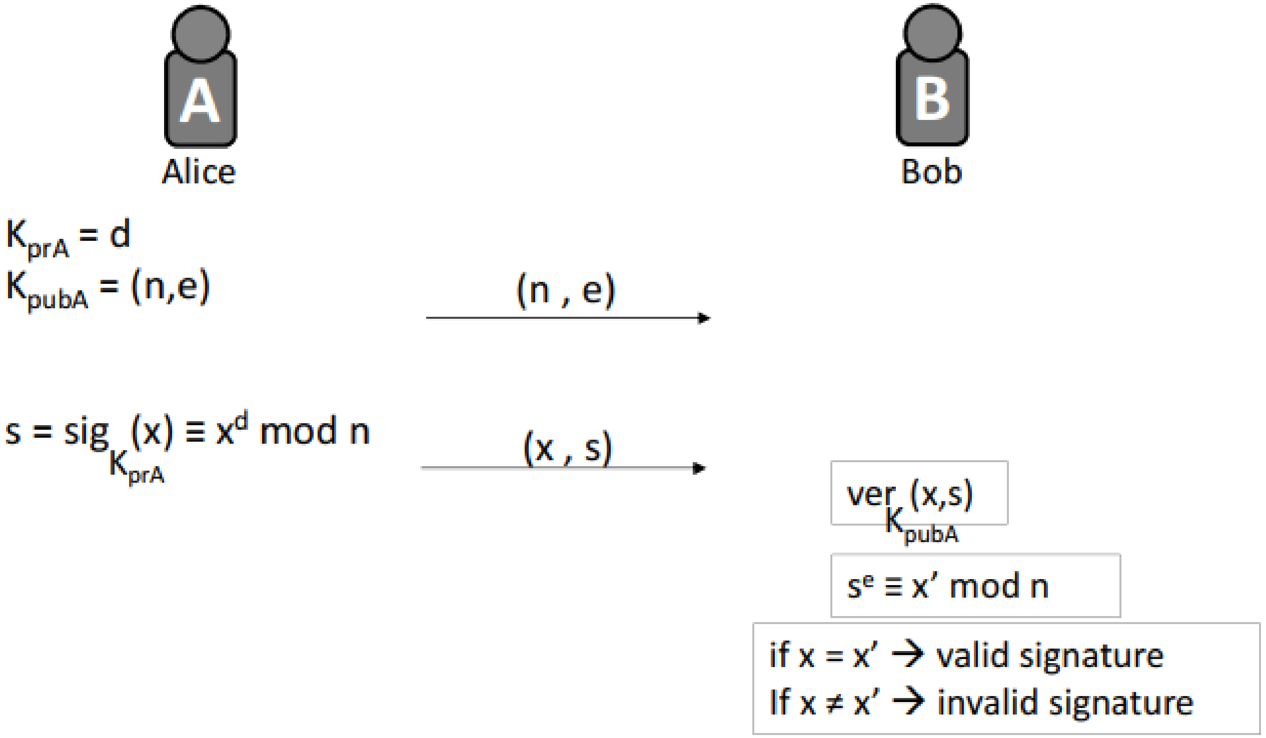
- Append *s* to message *x*

To verify the signature:

- “decrypt” the signature with the public key

$$\boxed{x' = ver_{K_{pub}}(s) = s^e \bmod n}$$

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. $d \equiv e^{-1} \equiv 7 \bmod 20$
	$\xleftarrow{(n,e)=(33,3)}$	
		compute signature for message $x = 4$: $s = x^d \equiv 4^7 \equiv 16 \bmod 33$
	$\xleftarrow{(x,s)=(4,16)}$	
verify: $x' = s^e \equiv 16^3 \equiv 4 \bmod 33$ $x' \equiv x \bmod 33 \Longrightarrow$ valid signature		

ElGamal Digital Signature

Key Generation for Elgamal Digital Signature

1. Choose a large prime p.
2. Choose a primitive element α of $\mathbb{Z}_p^*$ or a subgroup of $\mathbb{Z}_p^*$.
3. Choose a random integer $d \in \{2, 3, \ldots, p-2\}$.
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 $k_E \in \{0, 1, 2, \ldots, p-2\}$ 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

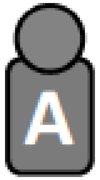
1. Compute the value

$$t \equiv \beta^r \cdot r^s \bmod p$$

2. The verification follows from:

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

ElGamal Digital Signature



Alice

Bob

Choose prime p

Choose primitive element α

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

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

$\xleftarrow{(\beta, p, \alpha)}$

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

$r \equiv \alpha^{K_E} \bmod p$

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

$\xleftarrow{x,\ (r,s)}$

Verify

$t \equiv \beta^r r^s \bmod p$

If $t \equiv \alpha^x \bmod p$ → valid sign

If $t \not\equiv \alpha^x \bmod p$ → invalid sign

ElGamal Digital Signature

Proof of correctness:

$\beta^r r^s \equiv (\alpha^d)^r(\alpha^{K_E})^s \bmod p$

$\equiv \alpha^{d.r+K_E.s} \bmod p \equiv \alpha^x \bmod p$

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

From Fermat's Little Theorem,

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

$a^m \bmod p \equiv a^r \bmod p$

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

So, $d.r+K_E.s \equiv x \bmod p-1$

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

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. $\beta = \alpha^d \equiv 7 \bmod 29$
	$\xleftarrow{(p,\alpha,\beta)=(29,2,7)}$	
		compute signature for message $x = 26$: choose $k_E = 5$, note that $\gcd(5,28) = 1$ $r = \alpha^{k_E} \equiv 2^5 \equiv 3 \bmod 29$ $s = (x - d\,r)\,k_E^{-1} \equiv (-10) \cdot 17 \equiv 26 \bmod 28$
	$\xleftarrow{(x,(r,s))=(26,(3,26))}$	
verify: $t = \beta^r \cdot r^s \equiv 7^3 \cdot 3^{26} \equiv 22 \bmod 29$ $\alpha^x \equiv 2^{26} \equiv 22 \bmod 29$ $t \equiv \alpha^x \bmod 29 \Longrightarrow$ valid signature		

Presentation Topics

- ➢Whirlpool Hash Function
- ➢Open-PGP CFB mode of operation
- ➢Attacks against Open-PGP CFB mode of operation
- ➢Homomorphic Encryption Algorithms
- ➢Secret Sharing Protocols
- ➢Chosen-prefix collision attack on SHA-1 Hash function

MSA UNIVERSITY
IN EGYPT SINCE 1996
Established by Dr.Nawal El Degwi
MSA UNIVERSITY
جامعة أكتوبر للعلوم الحديثة والآداب

Thank You!

See You next Lectures!!

Any Question?

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 **Hotline:** 16672 **Website:** www.msa.edu.eg