Cryptography
ECE5632 - Spring 2025

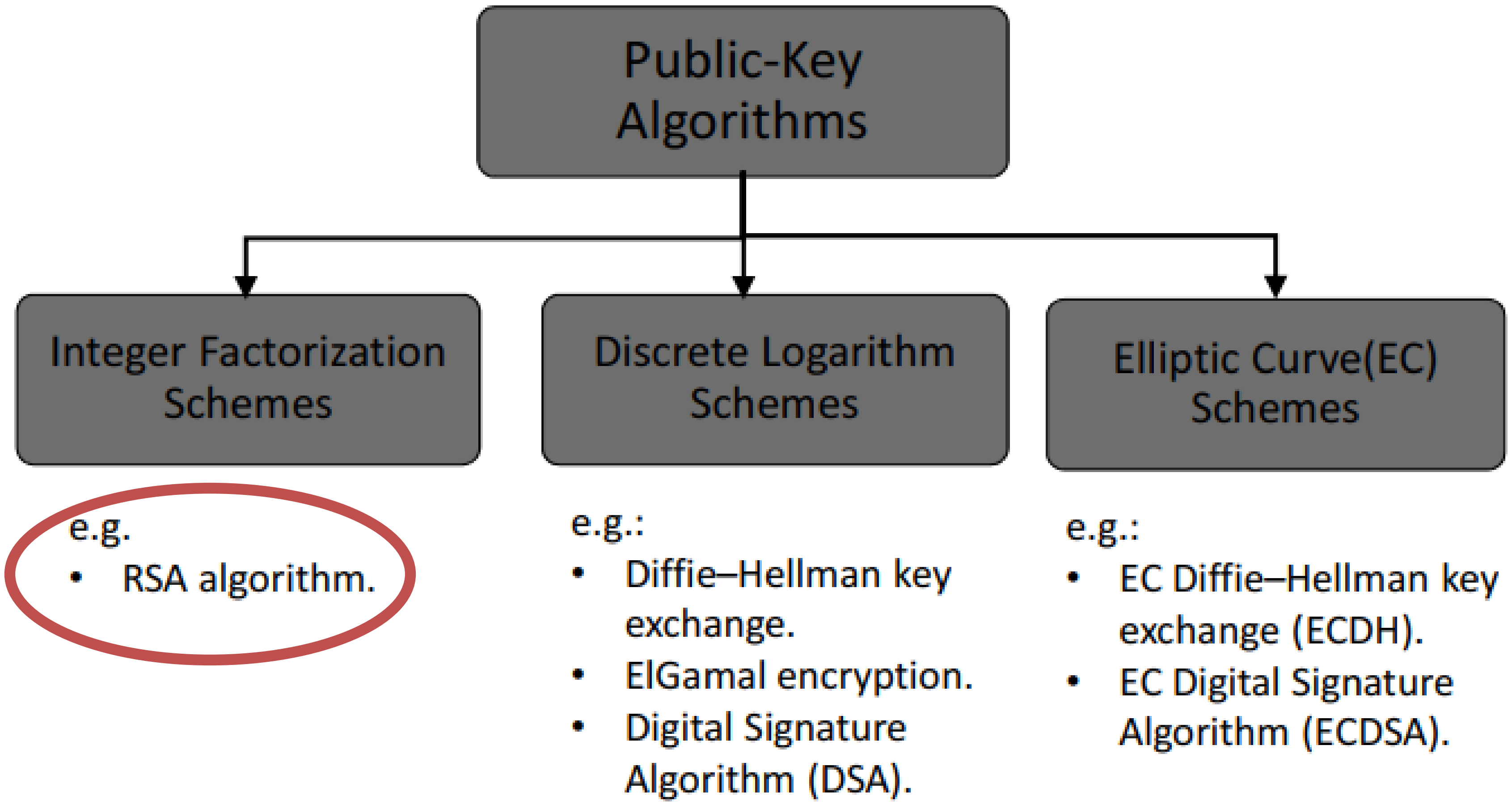
Lecture 7B

Dr. Farah Raad

Lecture Topic

RSA Algorithm & Diffie-Hellman Key

PKC Algorithms: Three Families



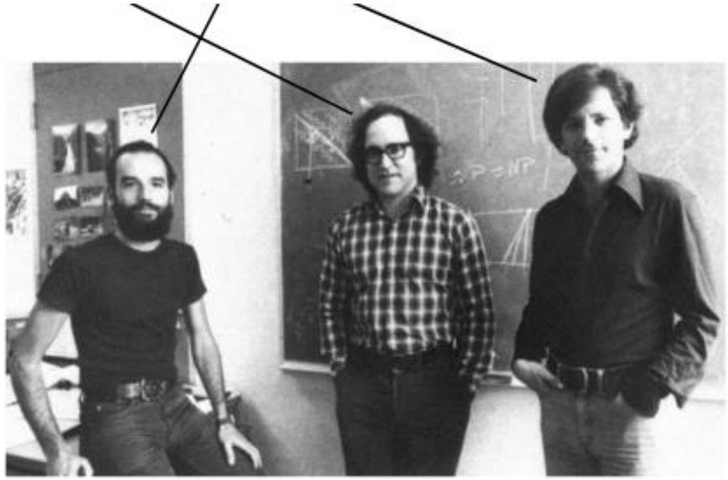
RSA Algorithm

➢ Some History

✓ 1976: Public key cryptography first introduced:

Martin Hellman and Whitfield Diffie published their landmark publickey paper in 1976

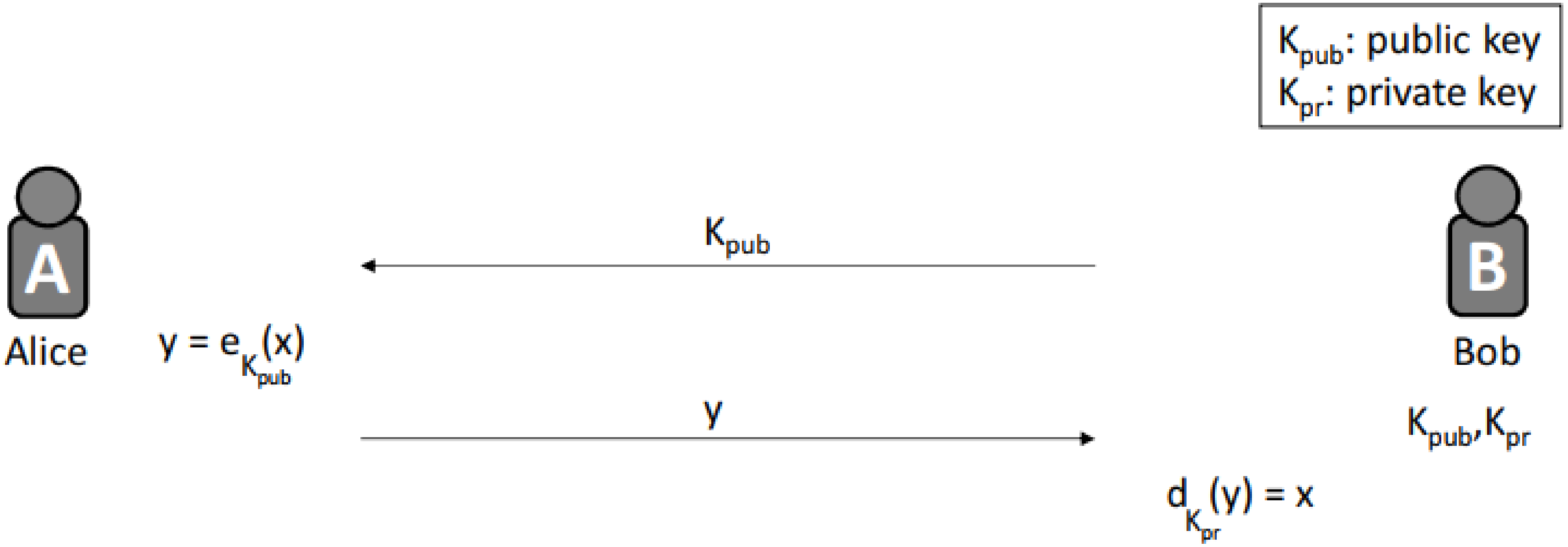
✓ 1977: **R**ivest–**S**hamir–**A**dleman (RSA) proposed the asymmetric RSA cryptosystem algorithm



✓ Until now, RSA is the most widely use asymmetric cryptosystem although elliptic curve cryptography (ECC) becomes increasingly popular

✓ RSA is mainly used for two applications
- Transport of (i.e., symmetric) keys
- Digital signatures

RSA Algorithm



1) How to encrypt/decrypt?
2) How to compute K_{pub} and K_{pr}?

RSA Algorithm

➢ Encryption and Decryption

- ✓ RSA operations are done over the integer ring Z_n (i.e., arithmetic modulo n), where $n = p * q$, with p, q being large primes
- ✓ Encryption and decryption are simply exponentiations in the ring
- ✓ In practice x, y, n and d are very long integer numbers (≥ 1024 bits)

Definition

Given the public key $(n,e) = k_{pub}$ and the private key $d = k_{pr}$ we write

$$y = e_{k_{pub}}(x) \equiv x^e \bmod n$$

$$x = d_{k_{pr}}(y) \equiv y^d \bmod n$$

where $x, y \in Z_n$.

We call $e_{k_{pub}}()$ the encryption and $d_{k_{pr}}()$ the decryption operation.

RSA Algorithm

➢ Key Generation

✓ Like all asymmetric schemes, RSA has set-up phase during which the private and public keys are computed

Algorithm: RSA Key Generation

Output: public key: $k_{pub} = (n, e)$ and private key $k_{pr} = d$

1. Choose two large primes p, q
2. Compute $n = p * q$
3. Compute $\Phi(n) = (p-1) * (q-1)$
4. Select the public exponent $e \in \{1, 2, \ldots, \Phi(n)-1\}$ such that gcd$(e, \Phi(n)) = 1$
5. Compute the private key d such that $d * e \equiv 1 \bmod \Phi(n)$
6. **RETURN** $k_{pub} = (n, e), k_{pr} = d$

RSA Algorithm

Remarks:

- Choosing two large, distinct primes *p, q* (in Step 1) is non-trivial
- gcd$(e, \Phi(n)) = 1$ ensures that *e* has an inverse and, thus, that there is always a private key *d*

Notes:

✓ In practice, n is ≥ 1024 bits long.
✓ Strength of RSA with n = $\mathbf{2^{3072}}$ is equivalent to AES128.
✓ Longer n means more security, but slower computation.
✓ p and q should differ in length by only a few digits . . . p, q ≥ 512 bits long

RSA Algorithm

Example: RSA with small numbers:

Alice

Message $x = 4$

$y = e_{K_{pub}}(x) \equiv x^e \bmod n$

$\equiv 4^3 \bmod 33$

$\equiv 31 \bmod 33$

Bob

1. $p=3,\ q=11$
2. $n = 33$
3. $\Phi(n) = (p-1) \cdot (q-1)$

   $= 2 \cdot 10 = 20$
4. Choose $e = 3$
5. $d \equiv e^{-1} \equiv 7 \bmod 20$

Bob → Alice: $K_{pub} = (33,3)$

Alice → Bob: y

$x = d_{K_{pr}}(y) \equiv y^d \bmod n$

$\equiv 31^7 \bmod 33$

$\equiv 4 \bmod 33$

RSA Algorithm

Parameters Example

Example of practical RSA parameters for n = 1024 →

$$
\begin{aligned}
p = {} & E0DFD2C2A288ACEBC705EFAB30E4447541A8C5A47A37185C5A9 \\
& CB98389CE4DE19199AA3069B404FD98C801568CB9170EB712BF \\
& 10B4955CE9C9DC8CE6855C6123_h \\
q = {} & EBE0FCF21866FD9A9F0D72F7994875A8D92E67AEE4B515136B2 \\
& A778A8048B149828AEA30BD0BA34B977982A3D42168F594CA99 \\
& F3981DDABFAB2369F229640115_h \\
n = {} & CF33188211FDF6052BDBB1A37235E0ABB5978A45C71FD381A91 \\
& AD12FC76DA0544C47568AC83D855D47CA8D8A779579AB72E635 \\
& D0B0AAAC22D28341E998E90F82122A2C06090F43A37E0203C2B \\
& 72E401FD06890EC8EAD4F07E686E906F01B2468AE7B30CBD670 \\
& 255C1FEDE1A2762CF4392C0759499CC0ABECFF008728D9A11ADF_h \\
e = {} & 40B028E1E4CCF07537643101FF72444A0BE1D7682F1EDB553E3 \\
& AB4F6DD8293CA1945DB12D796AE9244D60565C2EB692A89B888 \\
& 1D58D278562ED60066DD8211E67315CF89857167206120405B0 \\
& 8B54D10D4EC4ED4253C75FA74098FE3F7FB751FF5121353C554 \\
& 391E114C85B56A9725E9BD5685D6C9C7EED8EE442366353DC39_h \\
d = {} & C21A93EE751A8D4FBFD77285D79D6768C58EBF283743D2889A3 \\
& 95F266C78F4A28E86F545960C2CE01EB8AD5246905163B28D0B \\
& 8BAABB959CC03F4EC499186168AE9ED6D88058898907E61C7CC \\
& CC584D65D801CFE32DFC983707F87F5AA6AE4B9E77B9CE630E2 \\
& C0DF05841B5E4984D059A35D7270D500514891F7B77B804BED81_h
\end{aligned}
$$

RSA Algorithm

Proof of Correctness

We need to prove that $d_{Kpr}(e_{Kpub}(x)) = x$

i.e., prove that $(x^e)^d \equiv x^{de} \bmod n \equiv x \bmod n$

RSA Algorithm: Practical Consideration

RSA is a heavy user of exponentiation...

Encryption: $y = x^e \bmod n$

Decryption: $x = y^d \bmod n$

Problem: How to quickly exponentiate with extremely large numbers?

Solution: Using Square-and-Multiply Algorithm

e.g., x^{26}

Square	SQ	$x \cdot x = x^2$
Multiply	MUL	$x \cdot x^2 = x^3$
	SQ	$x^3 \cdot x^3 = x^6$
	SQ	$x^6 \cdot x^6 = x^{12}$
	MUL	$x \cdot x^{12} = x^{13}$
	SQ	$x^{13} \cdot x^{13} = x^{26}$

Represent the exponent in binary; x^{11010}

Initially start with x^1

$(x^1)^2 = x^{10}$

$(x^{10})x = x^{11}$

$(x^{11})^2 = x^{110}$

$(x^{110})^2 = x^{1100}$

$(x^{1100})x = x^{1101}$

$(x^{1101})^2 = x^{11010}$

Simply construct the binary exponent from left to right by shifting (SQ) and adding (MUL).

Note: MUL is only used for the 1 bits.

Looks random.. How do I know when to SQ and when to MUL?

Security of RSA

The RSA discussed so far is called **schoolbook RSA**.

It has several weaknesses:

- RSA is deterministic.
- $y=x$ for $x= 0, 1, -1$.
- RSA is malleable.

A malleable cipher allows an attackers to modify the value of x without decrypting y.

e.g., attacker wants to multiply x by s=2. But only has access to y and e.

Then replacing y with $s^e y$ leads to..

decryption: $(s^e y)^d \equiv s^{ed} x^{ed} \equiv sx \bmod n$.

In practice, these weaknesses can be eliminated by using padding.

i.e., Optimal Asymmetric Encryption Padding (OAEP)

Security of RSA: Attacks

Attack possibilities against RSA:

1. Protocol attacks
2. Mathematical attacks. i.e., factoring the modulus.

    The attackers knows n and e.

    But can't compute d because p and q are unknown!

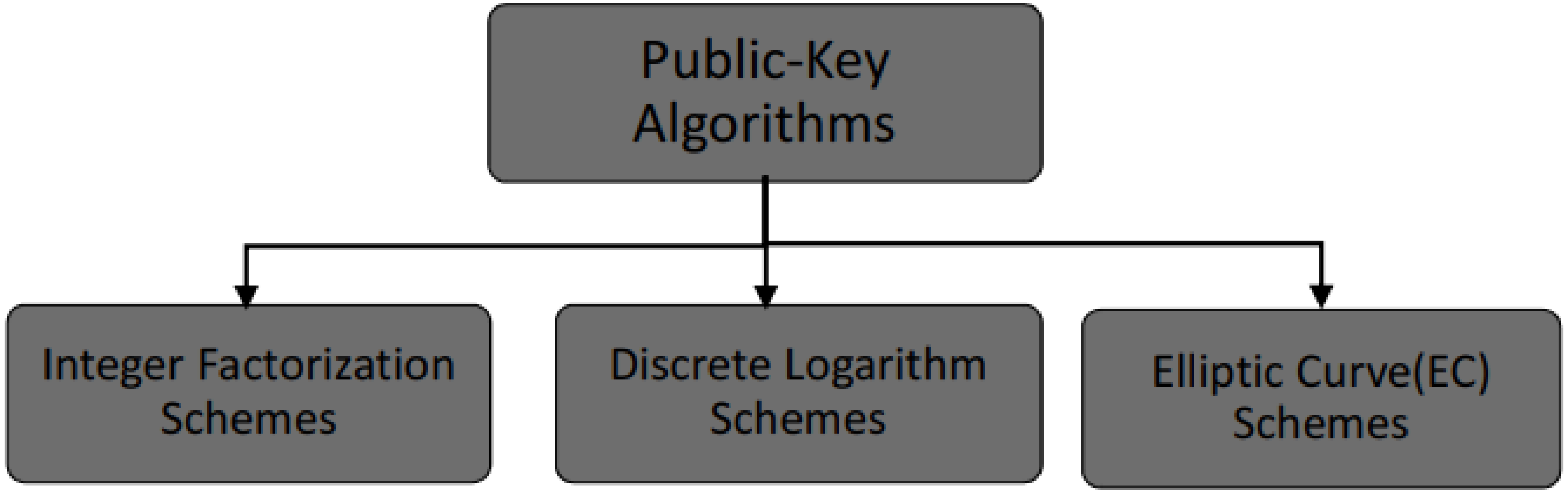
    Longer n is more difficult to factor, but slower algorithm.

    Minimum n size = 1024. Recommended 2048-4096.

3. Side-channel attacks.

    Exploit info leaked from the processing power or time (i.e., physical channels)

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).

Diffie-Hellman Key Exchange (DHKE)

- Proposed in 1976 by Whitfield Diffie and Martin Hellman
- Widely used, e.g. in Secure Shell (SSH), Transport Layer Security (TLS), and Internet Protocol Security (IPSec)
- The Diffie–Hellman Key Exchange (DHKE) is a key exchange protocol and not used for encryption
- (For the purpose of encryption based on the DHKE, ElGamal can be used.)

Diffie-Hellman Key Exchange (DHKE)

Diffie-Hellman setup:

1. Choose a large prime p.
2. Choose an integer $\alpha \in \{2,3,\ldots,p-2\}$.
3. Publish p and α.

p is a large prime ≥1024 bits long.
We'll soon discuss the nature of α.

Alice		Bob
Choose $a = k_{pr,A} \in \{2,\ldots,p-2\}$		Choose $b = k_{pr,B} \in \{2,\ldots,p-2\}$
Compute $A = k_{pub,A} \equiv \alpha^a \bmod p$	A →	Compute $B = k_{pub,B} \equiv \alpha^b \bmod p$
	← B	
$K_{AB} \equiv B^a \bmod p$		$K_{AB} \equiv A^b \bmod p$

As a result, K_{AB} is the shared secret.

e.g., we can use the 128 MSB of K_{AB} as a key for AES128.

Diffie-Hellman Key Exchange (DHKE)

Essential idea:

- Choose two random secrets **a** and **b**

$$(\alpha^a)^b \bmod p = (\alpha^b)^a \bmod p$$

- Both parties can calculate that value without sending secrets over the wire

Diffie-Hellman Key Exchange (DHKE)

Alice		Bob
Choose random private key $k_{prA}=a \in \{1,2,\ldots,p-1\}$		Choose random private key $k_{prB}=b \in \{1,2,\ldots,p-1\}$
Compute corresponding public key $k_{pubA}= A = \alpha^a \bmod p$	A →	
	← B	Compute correspondig public key $k_{pubB}= B = \alpha^b \bmod p$
Compute common secret $k_{AB} = B^a = (\alpha^a)^b \bmod p$		Compute common secret $k_{AB} = A^b = (\alpha^b)^a \bmod p$

We can now use the joint key k_{AB} for encryption, e.g., with AES

$y = AES_{kAB}(x)$	y →	$x = AES^{-1}_{kAB}(y)$

Diffie-Hellman Key Exchange (DHKE)

Example

Alice	Domain parameters	Bob
Choose random private key $a = 5$	$p=29$, $\alpha=2$	Choose random private key $b = 12$
Compute public key $A = \alpha^a = 2^5 = 3 \bmod 29$	A →	
	← B	Compute public key $B = \alpha^b = 2^{12} = 7 \bmod 29$
Compute common secret $k_{AB} = B^a = 7^5 = 16 \bmod 29$		Compute common secret $k_{AB} = A^b = 3^{12} = 16 \bmod 29$

Diffie-Hellman Key Exchange (DHKE)

So, . . . $K_{AB} \equiv B^a \bmod p \equiv A^b \bmod p$

$A \equiv \alpha^a \bmod p$
$B \equiv \alpha^b \bmod p$

How is that possible??

Proof:

$B^a \equiv (\alpha^b)^a \equiv \alpha^{ab} \bmod p$

$A^b \equiv (\alpha^a)^b \equiv \alpha^{ab} \bmod p$

Very simple. Very important.

α must be a <u>primitive element</u>.
What that means? Time for some math...

Groups

Cyclic Groups

Revisiting Groups

Group (G, ∘): a set of elements, with 1 group operator.

E.g., :
(G , +) additive group
(G, ×) multiplicative group

Has certain properties that must be satisfied:

A1. Closure:

If a and b belong to G, then a ∘ b is also in G.

A2. Associativity:

a ∘ (b ∘ c) = (a ∘ b) ∘ c for all a, b, c in G

M1…

etc. . .

- See Lecture 6A.

Revisiting Groups

Theorem 8.2.1
The set $\mathbb{Z}_n^*$ which consists of all integers $i = 0, 1, \ldots, n-1$ for which $\gcd(i, n) = 1$ forms an abelian group under multiplication modulo n. The identity element is $e = 1$.

Example Let us verify the validity of the theorem by considering the following example:

If we choose $n = 9$, $\mathbb{Z}_n^*$ consists of the elements $\{1, 2, 4, 5, 7, 8\}$.

Multiplication table for $\mathbb{Z}_9^*$

× mod 9	**1**	**2**	**4**	**5**	**7**	**8**
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

Revisiting Groups

Example : Is (Z_9 , ×) a multiplicative group?

Z_9 = {0, 1, 2, 3, 4, 5, 6, 7, 8}

Check for property A1, A2 , M1, etc..

.

.

Problem with inverse property: Inverses only exist for elements a; gcd(a,9)=1

∴ elements 0, 3, 6 have no inverse in Z_9.

So, we'll define a special set called Z_n^* , by simply removing noninvertible elements.

The elements of Z_n^* still satisfy all properties of a group.

i.e., Z_9^*= {1, 2, 4, 5, 7, 8} is a multiplicative group.

|G| = Order of G: The number of elements in G. . . . a.k.a. the cardinality of G.

$\therefore |Z_9^*| = 6$

Cyclic Groups

Definition 8.2.2 Finite Group
A group $(G, \circ)$ *is* finite *if it has a finite number of elements. We denote the* cardinality *or* order *of the group* G *by* $|G|$.

- $(\mathbb{Z}_n, +)$: the cardinality of $\mathbb{Z}_n$ is $|\mathbb{Z}_n| = n$ since $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$.
- $(\mathbb{Z}_n^*, \cdot)$: remember that $\mathbb{Z}_n^*$ is defined as the set of positive integers smaller than n which are relatively prime to n. Thus, the cardinality of $\mathbb{Z}_n^*$ equals Euler's phi function evaluated for n, i.e., $|\mathbb{Z}_n^*| = \Phi(n)$. For instance, the group $\mathbb{Z}_9^*$ has a cardinality of $\Phi(9) = 3^2 - 3^1 = 6$. This can be verified by the earlier example where we saw that the group consist of the six elements $\{1, 2, 4, 5, 7, 8\}$.

Cyclic Groups

Definition 8.2.3 Order of an element
The order $ord(a)$ *of an element* a *of a group* $(G, \circ)$ *is the smallest positive integer* k *such that*

$$a^k = \underbrace{a \circ a \circ \ldots \circ a}_{k\ times} = 1,$$

where 1 *is the identity element of* G.

- In the previous example, ord(3)=5.
- Don’t confuse ord(a) with |G|

Cyclic Groups

Example We try to determine the order of $a = 3$ in the group $\mathbb{Z}_{11}^*$. For this, we keep computing powers of a until we obtain the identity element 1.

$$
\begin{aligned}
a^1 &= 3 \\
a^2 &= a \cdot a \;\; = 3 \cdot 3 = 9 \\
a^3 &= a^2 \cdot a = 9 \cdot 3 = 27 \equiv 5 \bmod 11 \\
a^4 &= a^3 \cdot a = 5 \cdot 3 = 15 \equiv 4 \bmod 11 \\
a^5 &= a^4 \cdot a = 4 \cdot 3 = 12 \equiv 1 \bmod 11
\end{aligned}
$$

From the last line it follows that $\text{ord}(3) = 5$.

$$
\begin{aligned}
a^6 &= a^5 \cdot a \equiv 1 \cdot a \equiv 3 \bmod 11 \\
a^7 &= a^5 \cdot a^2 \equiv 1 \cdot a^2 \equiv 9 \bmod 11 \\
a^8 &= a^5 \cdot a^3 \equiv 1 \cdot a^3 \equiv 5 \bmod 11 \\
a^9 &= a^5 \cdot a^4 \equiv 1 \cdot a^4 \equiv 4 \bmod 11 \\
a^{10} &= a^5 \cdot a^5 \equiv 1 \cdot 1 \equiv 1 \bmod 11 \\
a^{11} &= a^{10} \cdot a \equiv 1 \cdot a \equiv 3 \bmod 11 \\
&\vdots
\end{aligned}
$$

the powers of a run through the sequence $\{3, 9, 5, 4, 1\}$

Cyclic Groups

In case of the multiplicative group Z_p^* , where p is prime;

$\therefore$ Z_p^*={1, 2, 3, …, p-1}

e.g., Z_{11}^*= {1, 2, 3, 4, 5, 6, 7, 8, 9, 10}

To understand what's cyclic groups,

let's pick a number (a=3) and compute all its powers..

$a^1=3$
$a^2=9$
$a^3=27 \equiv 5$
$a^4=a^3\,a=5 \times 3 \equiv 4$
$a^5= a^4\,a=4 \times 3 \equiv 1$
$a^6= a^5\,a=1 \times 3 \equiv 3$
$a^7= a^6\,a=3 \times 3 \equiv 9$

The result cycles over and over again.

Cyclic Groups

Definition 8.2.4 Cyclic Group
A group G which contains an element α with maximum order $ord(\alpha) = |G|$ is said to be cyclic. *Elements with maximum order are called* primitive elements *or* generators.

Cyclic Groups

Example We want to check whether $a = 2$ happens to be a primitive element of $\mathbb{Z}_{11}^* = \{1,2,3,4,5,6,7,8,9,10\}$.

$$\begin{aligned} a &= 2 & a^6 &\equiv 9 \bmod 11 \\ a^2 &= 4 & a^7 &\equiv 7 \bmod 11 \\ a^3 &= 8 & a^8 &\equiv 3 \bmod 11 \\ a^4 &\equiv 5 \bmod 11 & a^9 &\equiv 6 \bmod 11 \\ a^5 &\equiv 10 \bmod 11 & a^{10} &\equiv 1 \bmod 11 \end{aligned}$$

$$\mathrm{ord}(a) = 10 = |\mathbb{Z}_{11}^*|.$$

Note that the cardinality of the group is $|\mathbb{Z}_{11}^*| = 10$.

- Let's look again at all the elements that are generated by powers of two.

i	1	2	3	4	5	6	7	8	9	10
a^i	2	4	8	5	10	9	7	3	6	1

✓ The powers of $a = 2$ actually generate all elements of the group Z_{11}^*

Cyclic Groups

$Z_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$

$a^1 = 2$
$a^2 = 4$
$a^3 = 8$
$a^4 = 5$
$a^5 = 10$
$a^6 = 9$
$a^7 = 7$
$a^8 = 3$
$a^9 = 6$
$a^{10} = 1$
$a^{11} = 2$

Which elements did the number 2 **generate**? . . . All of them.
So, we call it a *generator*, primitive root, or a *primitive element*.

$\therefore$ ord(2)=10

a=2 is a generator of Z_{11}^*

$\therefore 2^{10} \bmod 11 \equiv 1$
$\therefore 2^{45363457210} \bmod 11 \equiv 1.$

❖ It is important to stress that the number 2 is not necessarily a generator in other cyclic groups

$$\mathbb{Z}_7^*, \operatorname{ord}(2) = 3$$

✓ The element 2 is thus not a generator in that group.

Cyclic Groups

- Cyclic Groups are the basis of several cryptosystems.
  - **For every prime p, (Z_p^* , ×) is a cyclic group.**

Theorem 8.2.2 *For every prime p, $(\mathbb{Z}_p^*, \cdot)$ is an abelian finite cyclic group.*

Theorem 8.2.3
Let G be a finite group. Then for every $a \in G$ it holds that:

1. $a^{|G|} = 1$
2. $ord(a)$ *divides* $|G|$

Cyclic Groups

Theorem 8.2.3
Let G be a finite group. Then for every $a \in G$ it holds that:

1. $a^{|G|} = 1$
2. $ord(a)$ *divides* $|G|$

- **Property 1:** Proof using Fermat's little theorem for Z_p^*

  $a^p \equiv a \bmod p$
  $a^{p-1} \equiv 1 \bmod p$
  $|Z_p^*| = p-1$
  $a^{p-1} = a^{|Z_p^*|} = 1$

- **Property 2:** example using Z_{11}^*

  $|Z_{11}^*| = 10$
  Possible orders $\in \{1, 2, 5, 10\}$

Cyclic Groups

Theorem 8.2.3
Let G be a finite group. Then for every $a \in G$ it holds that:

1. $a^{|G|} = 1$
2. $ord(a)$ *divides* $|G|$

- **Property 2:** example using Z_{11}^* *
  $| Z_{11}^* |$ = 10
  Possible orders ∈ {1, 2, 5, 10}
- How many primitive elements (i.e., generators) do we have?
- ✓ **Four elements: 2, 6, 7, 8.**
- ✓ The only element orders in this group are 1, 2, 5, and 10, since these are the only integers that divide 10.

ord(1) = 1
ord(2) = 10
ord(3) = 5
ord(4) = 5
ord(5) = 5
ord(6) = 10
ord(7) = 10
ord(8) = 10
ord(9) = 5
ord(10) = 2

Cyclic Groups

➢ **How is this related to DHKE?**

✓ Cyclic groups make good **Discrete Logarithm Problems.**

Definition: Discrete Logarithm Problem (DLP)
Given a prime p, an element $\beta \in Z_p^*$, and the generator α,

find x such that; $\alpha^x \equiv \beta \bmod p$

e.g., In DHKE, attackers know p, α, A, B
However, finding $K_{AB} = \alpha^{ab}$ is a hard problem. → Diffie-Hellman Problem (DHP)

Especially with a large p, attackers need to compute $\log_\alpha B \bmod p$.

Discrete Logarithm Problem (DLP)

Definition 8.3.1 Discrete Logarithm Problem (DLP) in $\mathbb{Z}_p^*$
Given is the finite cyclic group $\mathbb{Z}_p^*$ of order $p-1$ and a primitive element $\alpha \in \mathbb{Z}_p^*$ and another element $\beta \in \mathbb{Z}_p^*$. The DLP is the problem of determining the integer $1 \leq x \leq p-1$ such that:

$$\alpha^x \equiv \beta \mod p$$

$$x = \log_\alpha \beta \bmod p.$$

Discrete Logarithm Problem (DLP)

In other words…

If x is known, it's computationally easy to get $\alpha^x \equiv \beta \bmod p$

However, for large parameters, it's very difficult to get $\log_\alpha \beta \bmod p$

This forms a one-way function.

$2^x \equiv 36 \bmod 47$

$e.g., Z_{47}^{*}, \beta = 41, \alpha = 5$

Find x such that $5^x \equiv 41 \bmod 47$.

Using brute force, x = 15.

By using a brute-force attack, we obtain a solution for $x = 17$

Example: mod 7

➢ 3 is a **primitive element** or **generator** under the **multiplication** operation

$3^1 = 3 \bmod 7$

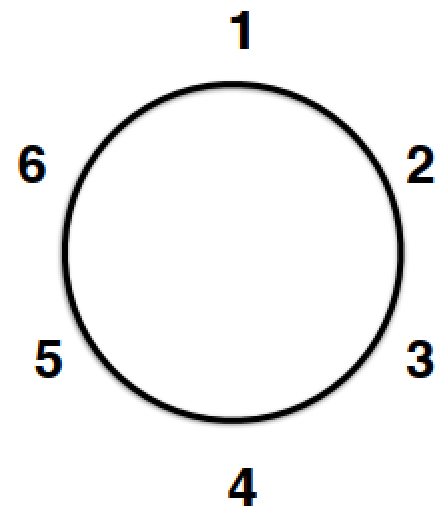
$3^2 = 9 = 2 \bmod 7$

$3^3 = 27 = 6 \bmod 7$

$3^4 = 81 = 4 \bmod 7$

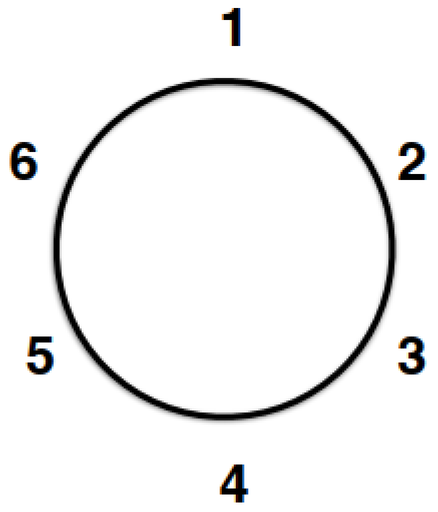
$3^5 = 243 = 5 \bmod 7$

$3^6 = 729 = 1 \bmod 7$



Example: mod 7

```
>>> for i in range(1,7):
...    print 3, "**", i, "= ", (3**i) % 7, "mod 7"
...
3 ** 1 =  3 mod 7
3 ** 2 =  2 mod 7
3 ** 3 =  6 mod 7
3 ** 4 =  4 mod 7
3 ** 5 =  5 mod 7
3 ** 6 =  1 mod 7
```

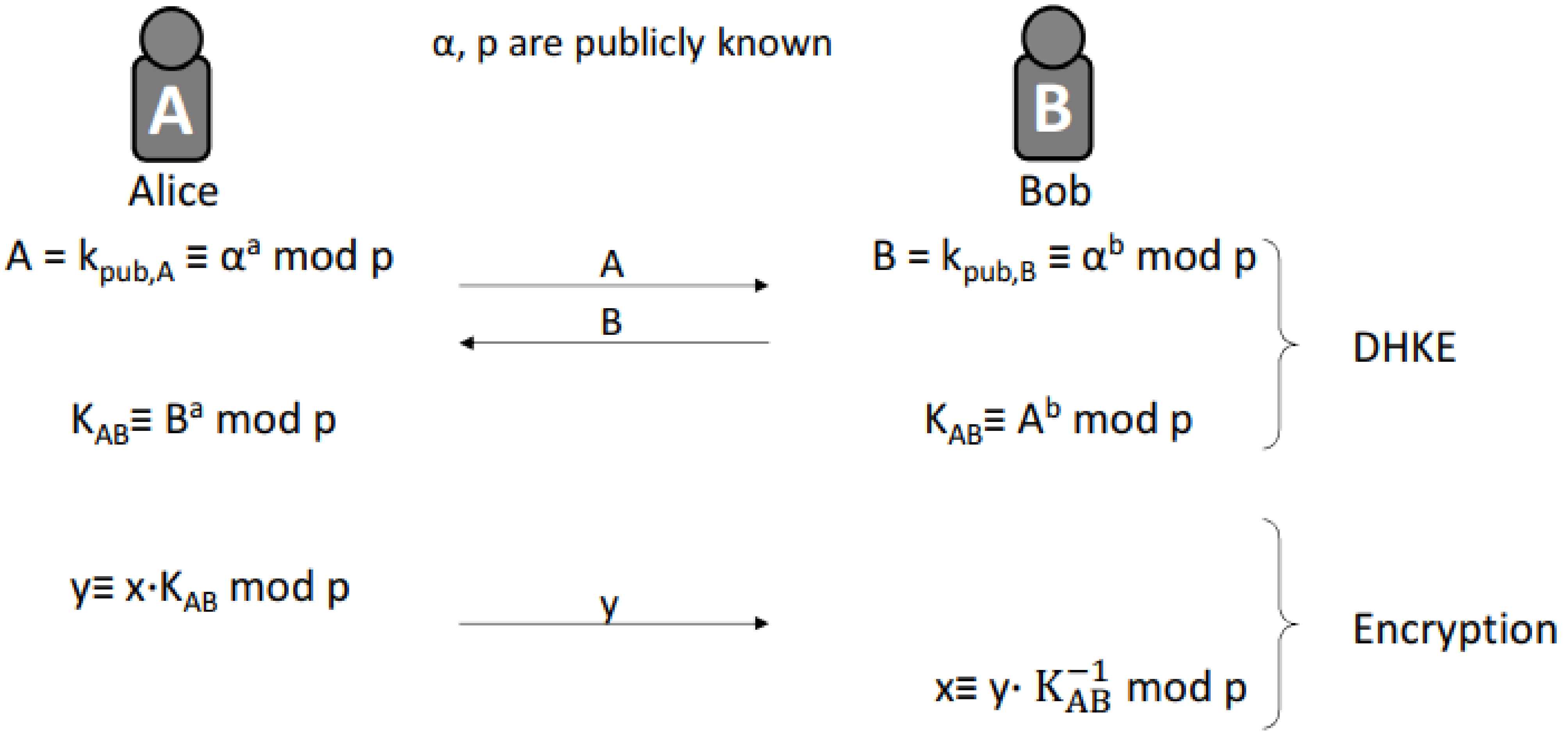


$\alpha = 3$

DLP: $3^x = 4 \bmod 7$ $\quad x = 4$

DLP: $3^x = 1 \bmod 7$ $\quad x = 6$

Concept of Encryption using DLP



Diffie-Hellman Problem (DHP)

Attackers know p, α, A, B
Attackers want $K_{AB} = \alpha^{ab}$

- Attacker's possible steps to solve DHP:
  1. Compute $a = \log_{\alpha} A \bmod p$
  2. Compute $B^a = K_{AB} \bmod p$

- For attackers, step 1 is computationally a very hard problem if p is large enough >1024 bits.

Security of DHKE

- DHKE alone is vulnerable to active attacks.
  - i.e., the protocol can be defeated if the attacker can modify the messages or generate false messages.
  - So, digital signatures and public-key certificates are used to overcome this vulnerability.
- Passive attacks.
  - Examples:
    - Exhaustive search
    - Index-calculus algorithm
    - Baby-step giant-step algorithm
    - Pollard’s rho algorithm
    - Pohlig–Hellman algorithm
  - To overcome, use large p

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