CSC3631 Cryptography
- Asymmetric Encryption II

Thomas Gross

1

Overview

Easy Land (Polynomial-Time)

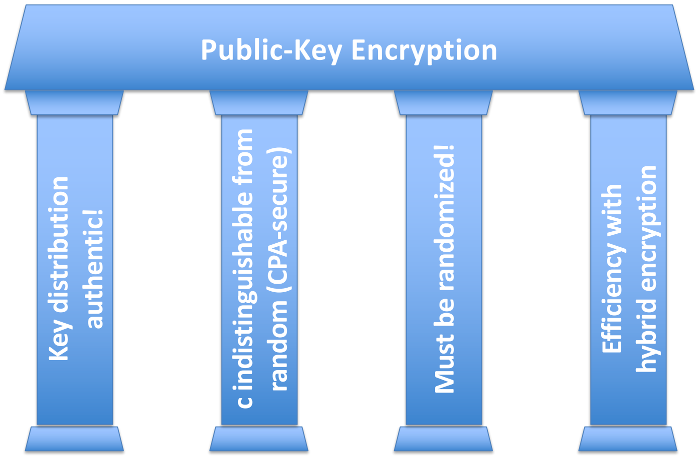
Addition:	a+b (mod N)	Multiplication:	a · b (mod N)
Inverse:	a^{-1} (mod N)	Exponentiation:	a^b (mod N)

Hard Land (Intractability)

Factoring	RSA	Discrete Log	Diffie-Hellman
What are p, q st. p · q = N?	What's x st. $x^e = y$ (**mod** N)?	What's x st. $g^x = h$ (mod p)	Distinguish g^{xy} from g^z
Integers	RSA Group $(Z_N)^*$, N=pq	Subgroups of $(Z_p)^*$	Subgroups of $(Z_p)^*$
Easy: Multiplication N = p · q	Easy: Exponentiation $x^e = y$ (**mod** N)	Easy: Exponentiation $g^x = h$ (mod p)	Easy: Exponentiation $K = g^{xy}$ (**mod** p)
Hard: Find factors of N	Hard: Find the e^{th} root x given y.	Hard: Find the discrete logarithm x given h.	Hard: Decide whether K is DH or random

2

Pillars of Public-key Encryption



3

Chosen-Plaintext Attack Security II

How can we formalize CPA indistinguishability?

Setup: Generate keypair (*pk*, *sk*)

→ *pk*, **Enc**$_{pk}$()

← candidate messages m_1, m_2

Choose random bit $b \leftarrow \{0,1\}$

Challenge ciphertext $c \leftarrow$ **Enc**$_{pk}(m_b)$

→ c

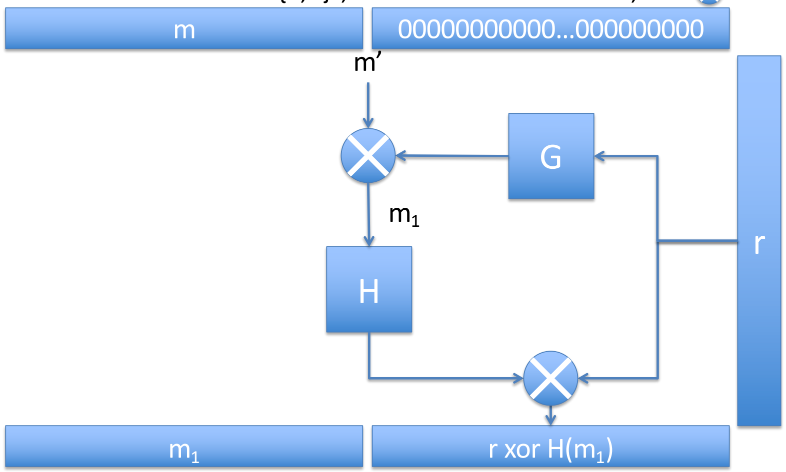
← a bit b'

Success criterion for **A:** if guess correct $b'=b$

4

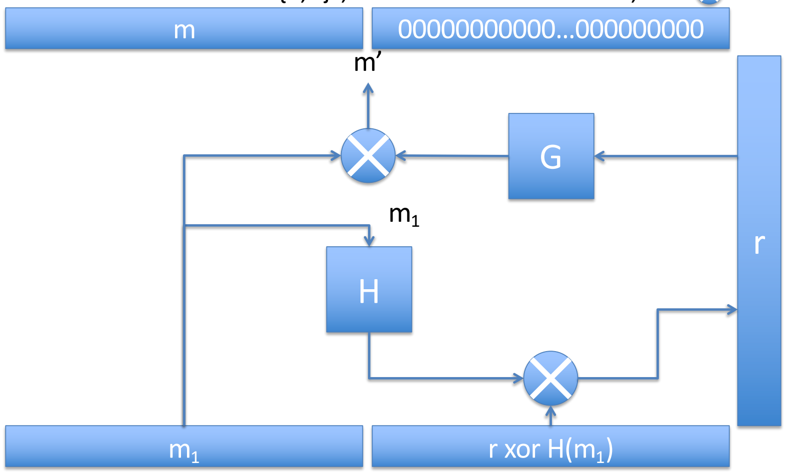
RSA OAEP

Choose random r in $\{0,1\}^n$; Hash-Functions **G** and **H**; XOR

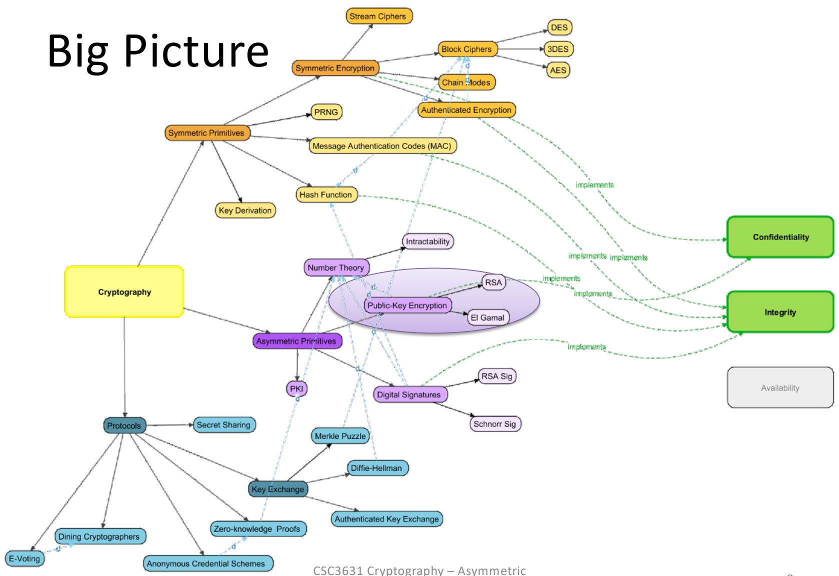


RSA OAEP Decryption

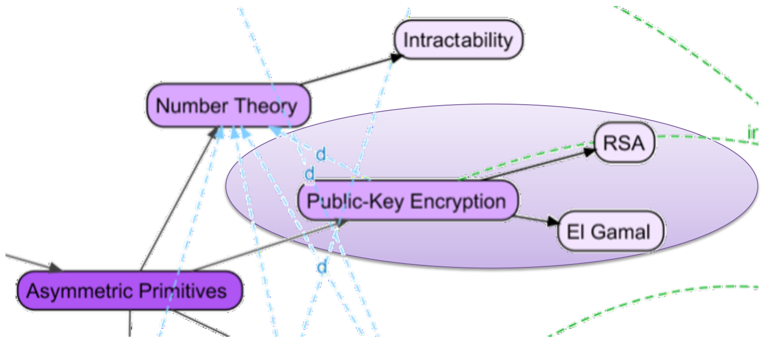
Choose random r in $\{0,1\}^n$; Hash-Functions **G** and **H**; XOR



Big Picture



Big Picture



Roadmap

- **El Gamal Encryption**
  - **Number Theory Foundations**
  - Underlying Assumptions
  - El Gamal
  - **Attacks on El Gamal**

Goal for today:

- **What is El Gamal?**
- **What can go wrong with El Gamal**

Blinding with a Random Element I Multiplication

Given a finite group *G* and a arbitrary element *m*

Choose a random *g* in *G*. Then $g' = m \cdot g$ is a **random element** of G again.

Example: $(Z_7)^*$ **random** $g = 5$

{ 1, 2, 3, 4, 5, 6 }

[Image Wikipedia]

Blinding with a Random Element II Exponentiation

Given a finite group *G* w/ generator *g* and order *q*.

Choose a random *x* in Z_q. Then $g' = g^x$ is a **random element** of *G* again.

Example: $(Z_7)^*$ 5^4 5^1 5^5 5^3

{ 1, 2, 3, 4, 5, 6 }

5^6 5^2

[Image Wikipedia]

Roadmap

- **El Gamal Encryption**
  - Number Theory Foundations
  - **Underlying Assumptions**
  - El Gamal
  - Attacks on El Gamal

Goal for today:

- **What is El Gamal?**
- **What can go wrong with El Gamal**

What is the Discrete Logarithm?

Given a h in $(\mathbf{Z}_p)^*$ with generator g,

find the x such that

$g^x = h \quad (\textbf{mod } p)$

Example: $(\mathbf{Z}_{17})^*$, g=3

{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16}

The Discrete Logarithm Assumption*

What's the basis of the DH and El Gamal crypto systems?

Setup: $((\mathbf{Z}_p)^*, q, g) \leftarrow$ **GenGroup**(1^n), where q = **ord**(*g*)

Choose h from $(\mathbf{Z}_p)^*$ by $h = g^{x'}$ (**mod** p)

Input for Adversary **A**: $(\mathbf{Z}_p)^*, q, g, h$

Output of Adversary **A**: x in $\mathbf{Z}_q$

Adversary A success: if $g^x = h$ (**mod** N)

The Discrete Logarithm problem is **hard** relative to GenGroup if all probabilistic and polynomial-time adversaries **A** only have negligible success probability.

[*) The Discrete Logarithm Assumption holds in arbitrary cyclic groups or order q.]

Decisional Diffie-Hellman Assumption*

What's the basis of the Diffie-Hellman key exchange?

Setup: $((\mathbf{Z}_p)^*, q, g) \leftarrow$ **GenGroup**(1^n), where q = **ord**(*g*)

Compute $h_1 = g^x$ (**mod** p) and $h_2 = g^y$ (**mod** p)

Input for Adversary **A**: $(\mathbf{Z}_p)^*, q, g, h_1, h_2, K$ where $K = g^z$ or $K = g^{xy}$

Output of Adversary **A**: Decision for g^z or g^{xy}

Adversary A success: if guessed type of K

The Decisional Diffie Hellman problem is **hard** relative to GenGroup if all probabilistic and polynomial-time adversaries **A** only have negligible success probability to distinguish g^{xy} from a random number.

[*) In the key exchange lecture, we only considered the Computational Diffie-Hellman, as simplification.]

Roadmap

- **El Gamal Encryption**
  - Number Theory Foundations
  - Underlying Assumptions
  - **El Gamal**
  - Attacks on El Gamal

Goal for today:

- **What is El Gamal?**
- **What can go wrong with El Gamal**

El Gamal Key Generation

How to create a strong setting for El Gamal?

GenElGamal(1^n)

Input: key length n

Create a cyclic group G (e.g. in $(\mathbf{Z}_p)^*$)
with order q and generator g.

Choose random x in $\mathbf{Z}_q$

Compute $h = g^x$ (**mod** q)

Output: $pk=(G, q, g, h)$, $sk=(G, q, g, x)$

El Gamal Encryption (e.g. in $(\mathbf{Z}_p)^*$)

KeyGen: $pk=(G, q, g, h)$, $sk=(G, q, g, x) \leftarrow$ **GenElGamal**(1^n)

Enc: Given pk=(G, q, g, h) and a message m:

Choose random y in $\mathbf{Z}_q$

Ciphertext: $(c_1=g^y, c_2=h^y \cdot m)$

Dec: Given sk=(G, q, g, x) and ciphertext (c_1, c_2):

$$m = c_2 \cdot (c_1^x)^{-1}$$

Correctness of El Gamal

Ciphertext: $(c_1=g^y, c_2=h^y \cdot m)$ **Message:** $m = c_2 \cdot (c_1^x)^{-1}$

Correctness of El Gamal

Ciphertext: $(c_1=g^y, c_2=h^y \cdot m)$ **Message:** $m = c_2 \cdot (c_1^x)^{-1}$

$$\begin{aligned}
c_2 \cdot (c_1^x)^{-1} &= (h^y \cdot m) \cdot (c_1^x)^{-1} && \text{| Subst. } c_2=h^y \cdot m \\
&= ((g^x)^y \cdot m) \cdot (c_1^x)^{-1} && \text{| Subst. } h = g^y \\
&= (g^{xy} \cdot m) \cdot (c_1^x)^{-1} \\
&= (g^{xy} \cdot m) \cdot ((g^y)^x)^{-1} && \text{| Subst. } c_1 = g^y \\
&= (g^{xy} \cdot m) \cdot (g^{yx})^{-1} && \text{| Exp. commute} \\
&= g^{xy} \cdot m \cdot (g^{xy})^{-1} \\
&= \cancel{g^{xy}} \cdot m \cdot (\cancel{g^{xy}})^{-1} = m && \text{| Mult. inverse}
\end{aligned}$$

■

Example of El Gamal

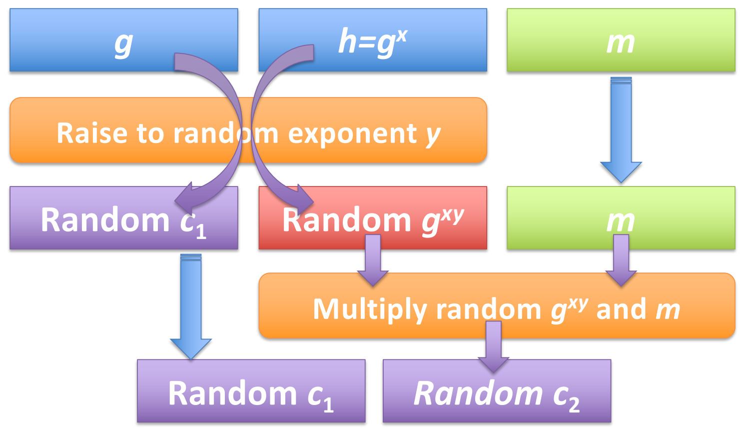
GenElGamal: prime $p = 2357$, generator $g = 2$ of $(\mathbf{Z}_{2357})^*$
Private key $x = 1751$.
Public key $h = g^x$ (**mod** p) = 2^{1751} (**mod** 2357) = 1185

Encryption: Message $m = 2035$, select random $y = 1520$
$c_1 = g^y$ (**mod** p) = 2^{1520} (**mod** p) = 1430
$c_2 = h^y \cdot m$ (**mod** p) = $1185^{1520} \cdot 2035$ (**mod** 2357) = 697

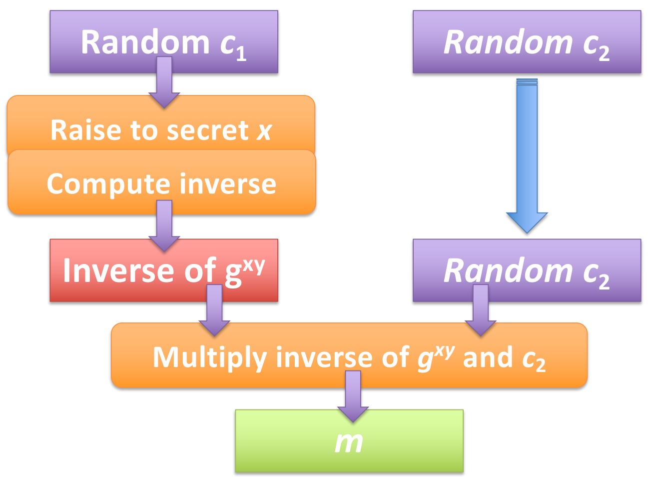
Decryption: Ciphertext $c_1 = 1430$, $c_2 = 697$
$m = c_2 \cdot c_1^{x}$ (**mod** p) = $697 \cdot (1430^{1751})^{-1}$ (**mod** 2357) = 2035

[Example adapted from Menezes et al., Handbook of Applied Cryptography]

El Gamal Encryption Graphically



El Gamal Decryption Graphically



Roadmap

- **El Gamal Encryption**
  - Number Theory Foundations
  - Underlying Assumptions
  - El Gamal
  - **Attacks on El Gamal**

Goal for today:
- **What is El Gamal?**
- **What can go wrong with El Gamal**

Attacks on Weak Randomness

Critical to use **different** y in each encryption.

What can go wrong?

Comparison RSA and El Gamal

RSA	El Gamal
Deterministic	Randomized
$(\mathbf{Z}_N)^*$, $N=pq$	$(\mathbf{Z}_p)^*$
Enc: 1 exp, Dec: 1 exp	Enc: 2 exp, Dec: 1 exp
Factoring RSA Problem	Discrete Log Problem Diffie-Hellman Problem