Groups for PKE: A Quick Primer

Discrete Log and DDH Assumptions,
Candidate Trapdoor One-Way Permutations

Groups, a primer

Groups, a primer

- A set G (for us finite, unless otherwise specified)

Groups, a primer

- A set G (for us finite, unless otherwise specified)
- A binary operation $*$: $G \times G \to G$

Groups, a primer

- A set G (for us finite, unless otherwise specified)
- A binary operation *: G×G→G

Abuse of notation:
G instead of (G,*)

Groups, a primer

- A set G (for us finite, unless otherwise specified)
- A binary operation *: G×G→G
  - Sometimes called addition, sometimes called multiplication (depending on the set/operation)

Abuse of notation:
G instead of (G,*)

Groups, a primer

- A set G (for us finite, unless otherwise specified)
- A binary operation *: $G \times G \to G$

Abuse of notation:
G instead of (G,*)

  - Sometimes called addition, sometimes called multiplication (depending on the set/operation)
  - Properties:

Groups, a primer

- A set G (for us finite, unless otherwise specified)
- A binary operation *: G×G→G
  - Sometimes called addition, sometimes called multiplication (depending on the set/operation)
  - Properties: Associativity,

Abuse of notation:
G instead of (G,*)

Groups, a primer

- A set G (for us finite, unless otherwise specified)
- A binary operation *: G×G→G
  - Sometimes called addition, sometimes called multiplication (depending on the set/operation)
  - Properties: Associativity, Existence of identity,

Abuse of notation:
G instead of (G,*)

Groups, a primer

- A set G (for us finite, unless otherwise specified)
- A binary operation *: G×G→G

Abuse of notation:
G instead of (G,*)

  - Sometimes called addition, sometimes called multiplication (depending on the set/operation)
  - Properties: Associativity, Existence of identity, Invertibility

Groups, a primer

- A set G (for us finite, unless otherwise specified)
- A binary operation *: G×G→G

Abuse of notation:
G instead of (G,*)

  - Sometimes called addition, sometimes called multiplication (depending on the set/operation)
  - Properties: Associativity, Existence of identity, Invertibility
    - Also for us (unless specified otherwise) Commutativity

Groups, a primer

- A set G (for us finite, unless otherwise specified)
- A binary operation *: $G \times G \to G$

Abuse of notation:
G instead of (G,*)

  - Sometimes called addition, sometimes called multiplication (depending on the set/operation)
  - Properties: Associativity, Existence of identity, Invertibility
    - Also for us (unless specified otherwise) Commutativity
  - Examples: $\mathbb{Z}$ (integers, with addition operation; infinite group), $\mathbb{Z}_N$ (integers modulo N), G^n (G group; coordinate-wise op)

Groups, a primer

Groups, a primer

- Computation with groups

Groups, a primer

- Computation with groups
  - For us, finite, but typically large: i.e., exponential in k

Groups, a primer

- Computation with groups
  - For us, finite, but typically large: i.e., exponential in k
  - Some compact representation of the elements (poly(k) bits)

Groups, a primer

- Computation with groups
  - For us, finite, but typically large: i.e., exponential in k
  - Some compact representation of the elements (poly(k) bits)
  - Efficient algorithms for:

Groups, a primer

- Computation with groups
  - For us, finite, but typically large: i.e., exponential in k
  - Some compact representation of the elements (poly(k) bits)
  - Efficient algorithms for:
    - Checking if an element (in standard rep.) is in the group

Groups, a primer

- Computation with groups
  - For us, finite, but typically large: i.e., exponential in k
  - Some compact representation of the elements (poly(k) bits)
  - Efficient algorithms for:
    - Checking if an element (in standard rep.) is in the group
    - Group operation (on elements in standard rep.)

Groups, a primer

- Computation with groups
  - For us, finite, but typically large: i.e., exponential in k
  - Some compact representation of the elements (poly(k) bits)
  - Efficient algorithms for:
    - Checking if an element (in standard rep.) is in the group
    - Group operation (on elements in standard rep.)
    - Inverting

Groups, a primer

- Computation with groups
  - For us, finite, but typically large: i.e., exponential in k
  - Some compact representation of the elements (poly(k) bits)
  - Efficient algorithms for:
    - Checking if an element (in standard rep.) is in the group
    - Group operation (on elements in standard rep.)
    - Inverting
    - Sampling a random element (almost) uniformly

Groups, a primer

- Computation with groups
  - For us, finite, but typically large: i.e., exponential in k
  - Some compact representation of the elements (poly(k) bits)
  - Efficient algorithms for:
    - Checking if an element (in standard rep.) is in the group
    - Group operation (on elements in standard rep.)
    - Inverting
    - Sampling a random element (almost) uniformly
  - Group itself represented by these algorithms

Groups, a primer

- Computation with groups
  - For us, finite, but typically large: i.e., exponential in k
  - Some compact representation of the elements (poly(k) bits)
  - Efficient algorithms for:
    - Checking if an element (in standard rep.) is in the group
    - Group operation (on elements in standard rep.)
    - Inverting
    - Sampling a random element (almost) uniformly
  - Group itself represented by these algorithms
- For collection of groups: GroupGen, an algorithm to select a group

Groups, a primer

Groups, a primer

- Additive notation: X+Y, identity denoted as 0, X+X denoted by 2X

Groups, a primer

- Additive notation: X+Y, identity denoted as 0, X+X denoted by 2X
- Multiplicative notation: XY, identity 1, XX denoted as X^2

Groups, a primer

- Additive notation: X+Y, identity denoted as 0, X+X denoted by 2X
- Multiplicative notation: XY, identity 1, XX denoted as X^2
- Order of a group G: |G| = number of elements in G

Groups, a primer

- Additive notation: X+Y, identity denoted as 0, X+X denoted by 2X
- Multiplicative notation: XY, identity 1, XX denoted as X^2
- Order of a group G: |G| = number of elements in G
- Cyclic group (finite, in multiplicative notation): there is one element g such that $G = \{g^0, g^1, g^2, \ldots g^{|G|-1}\}$

Groups, a primer

- Additive notation: X+Y, identity denoted as 0, X+X denoted by 2X
- Multiplicative notation: XY, identity 1, XX denoted as X^2
- Order of a group G: |G| = number of elements in G
- Cyclic group (finite, in multiplicative notation): there is one element g such that $G = \{g^0, g^1, g^2, \ldots g^{|G|-1}\}$

Groups, a primer

- Additive notation: X+Y, identity denoted as 0, X+X denoted by 2X
- Multiplicative notation: XY, identity 1, XX denoted as X^2
- Order of a group G: |G| = number of elements in G
- Cyclic group (finite, in multiplicative notation): there is one element g such that $G = \{g^0, g^1, g^2, \ldots g^{|G|-1}\}$

Groups, a primer

- Additive notation: X+Y, identity denoted as 0, X+X denoted by 2X
- Multiplicative notation: XY, identity 1, XX denoted as X^2
- Order of a group G: |G| = number of elements in G
- Cyclic group (finite, in multiplicative notation): there is one element g such that G = $\{g^0, g^1, g^2, \ldots g^{|G|-1}\}$

Groups, a primer

- Additive notation: X+Y, identity denoted as 0, X+X denoted by 2X
- Multiplicative notation: XY, identity 1, XX denoted as X^2
- Order of a group G: |G| = number of elements in G
- Cyclic group (finite, in multiplicative notation): there is one element g such that G = $\{g^0, g^1, g^2, \ldots g^{|G|-1}\}$

Groups, a primer

- Additive notation: X+Y, identity denoted as 0, X+X denoted by 2X
- Multiplicative notation: XY, identity 1, XX denoted as X^2
- Order of a group G: |G| = number of elements in G
- Cyclic group (finite, in multiplicative notation): there is one element g such that G = $\{g^0, g^1, g^2, \ldots g^{|G|-1}\}$

Groups, a primer

- Additive notation: X+Y, identity denoted as 0, X+X denoted by 2X
- Multiplicative notation: XY, identity 1, XX denoted as X^2
- Order of a group G: |G| = number of elements in G
- Cyclic group (finite, in multiplicative notation): there is one element g such that G = $\{g^0, g^1, g^2, \ldots g^{|G|-1}\}$

Groups, a primer

- Additive notation: X+Y, identity denoted as 0, X+X denoted by 2X
- Multiplicative notation: XY, identity 1, XX denoted as X^2
- Order of a group G: |G| = number of elements in G
- Cyclic group (finite, in multiplicative notation): there is one element g such that G = $\{g^0, g^1, g^2, \ldots g^{|G|-1}\}$
  - e.g. $\mathbb{Z}_N$, with say g=1 (additive group)

Groups, a primer

- Additive notation: X+Y, identity denoted as 0, X+X denoted by 2X
- Multiplicative notation: XY, identity 1, XX denoted as X^2
- Order of a group G: |G| = number of elements in G
- Cyclic group (finite, in multiplicative notation): there is one element g such that G = $\{g^0, g^1, g^2, \ldots g^{|G|-1}\}$
  - e.g. $\mathbb{Z}_N$, with say g=1 (additive group)
    - or any g s.t. gcd(g,N) = 1

Groups, a primer

- Additive notation: X+Y, identity denoted as 0, X+X denoted by 2X
- Multiplicative notation: XY, identity 1, XX denoted as X^2
- Order of a group G: |G| = number of elements in G
- Cyclic group (finite, in multiplicative notation): there is one element g such that G = $\{g^0, g^1, g^2, \ldots g^{|G|-1}\}$
  - e.g. $\mathbb{Z}_N$, with say g=1 (additive group)
    - or any g s.t. gcd(g,N) = 1
  - Number of generators of $\mathbb{Z}_N$ =: $\varphi(N)$

Groups, by examples

Groups, by examples

- $\mathbb{Z}_N^*$ = (generators of $\mathbb{Z}_N$, multiplication mod N)

Groups, by examples

- $\mathbb{Z}_N^*$ = (generators of $\mathbb{Z}_N$, multiplication mod N)
  - Numbers which have multiplicative inverse mod N

Groups, by examples

- $\mathbb{Z}_N^*$ = (generators of $\mathbb{Z}_N$, multiplication mod N)
  - Numbers which have multiplicative inverse mod N
  - If N is prime, $\mathbb{Z}_N^*$ is a cyclic group, of order N-1

Groups, by examples

- $\mathbb{Z}_N^*$ = (generators of $\mathbb{Z}_N$, multiplication mod N)
  - Numbers which have multiplicative inverse mod N
  - If N is prime, $\mathbb{Z}_N^*$ is a cyclic group, of order N-1
    - e.g. $\mathbb{Z}_5^*$ = {1,2,3,4} is generated by 2 (as {1,2,4,3}), and by 3 (as {1,3,4,2})

Groups, by examples

- $\mathbb{Z}_N^*$ = (generators of $\mathbb{Z}_N$, multiplication mod N)
  - Numbers which have multiplicative inverse mod N
  - If N is prime, $\mathbb{Z}_N^*$ is a cyclic group, of order N-1
    - e.g. $\mathbb{Z}_5^*$ = {1,2,3,4} is generated by 2 (as {1,2,4,3}), and by 3 (as {1,3,4,2})
    - (Also cyclic for certain other values of N)

Discrete Log

Discrete Log

- Discrete Log (w.r.t g) in a (multiplicative) group G generated by g:
  $DL_g(X)$ = unique x such that $X = g^x$ ($x \in \{0,1,\ldots,|G|-1\}$)

Discrete Log

- Discrete Log (w.r.t g) in a (multiplicative) group G generated by g:
  $DL_g(X)$ = unique x such that $X = g^x$ ($x \in \{0,1,\ldots,|G|-1\}$)
  - This could be used as a compact representation of elements in G

Discrete Log

- Discrete Log (w.r.t g) in a (multiplicative) group G generated by g:
  $DL_g(X)$ = unique x such that $X = g^x$ ($x \in \{0,1,\ldots,|G|-1\}$)
  - This could be used as a compact representation of elements in G
    - Group operation is given by $\mathbb{Z}_{|G|}$ operations on the discrete logs

Discrete Log

- Discrete Log (w.r.t g) in a (multiplicative) group G generated by g:
  $DL_g(X)$ = unique x such that $X = g^x$ ($x \in \{0,1,\ldots,|G|-1\}$)
  - This could be used as a compact representation of elements in G
    - Group operation is given by $\mathbb{Z}_{|G|}$ operations on the discrete logs
  - But may also consider the group with a different representation (e.g. natural representation for $\mathbb{Z}_p^*$)

Discrete Log

- Discrete Log (w.r.t g) in a (multiplicative) group G generated by g:
  $DL_g(X)$ = unique x such that $X = g^x$ ($x \in \{0,1,\ldots,|G|-1\}$)
  - This could be used as a compact representation of elements in G
    - Group operation is given by $\mathbb{Z}_{|G|}$ operations on the discrete logs
  - But may also consider the group with a different representation (e.g. natural representation for $\mathbb{Z}_p^*$)
- In a computational group, given standard representation of g and x, can efficiently find the standard representation of $X=g^x$ (How?)

Discrete Log

- Discrete Log (w.r.t g) in a (multiplicative) group G generated by g:
  $DL_g(X)$ = unique x such that $X = g^x$ ($x \in \{0,1,\ldots,|G|-1\}$)
  - This could be used as a compact representation of elements in G
    - Group operation is given by $\mathbb{Z}_{|G|}$ operations on the discrete logs
  - But may also consider the group with a different representation (e.g. natural representation for $\mathbb{Z}_p^*$)
- In a computational group, given standard representation of g and x, can efficiently find the standard representation of $X=g^x$ (How?)
  - But given X and g, may not be easy to find x (depending on G)

Discrete Log Assumption

Discrete Log Assumption

- In several groups, PPT adversaries are assumed to have negligible probability of solving the discrete logarithm problem

Discrete Log Assumption

- In several groups, PPT adversaries are assumed to have negligible probability of solving the discrete logarithm problem
  - Probability over choice of the group (from a collection), of a generator, and a random group element X

Discrete Log Assumption

- In several groups, PPT adversaries are assumed to have negligible probability of solving the discrete logarithm problem
  - Probability over choice of the group (from a collection), of a generator, and a random group element X
    - DL Expt: $(G,g) \leftarrow \text{GroupGen}$; $X \leftarrow G$; $\text{Adv}(G,g,X) \rightarrow z$; $g^z = X$?

Discrete Log Assumption

- In several groups, PPT adversaries are assumed to have negligible probability of solving the discrete logarithm problem
  - Probability over choice of the group (from a collection), of a generator, and a random group element X
    - DL Expt: $(G,g) \leftarrow \text{GroupGen}$; $X \leftarrow G$; $\text{Adv}(G,g,X) \rightarrow z$; $g^z = X$?
  - If Eve could solve the discrete logarithm (DL) problem, then Diffie-Hellman key-exchange is no good

Discrete Log Assumption

- In several groups, PPT adversaries are assumed to have negligible probability of solving the discrete logarithm problem
  - Probability over choice of the group (from a collection), of a generator, and a random group element X
    - DL Expt: $(G,g) \leftarrow \text{GroupGen}$; $X \leftarrow G$; $\text{Adv}(G,g,X) \rightarrow z$; $g^z = X$?
  - If Eve could solve the discrete logarithm (DL) problem, then Diffie-Hellman key-exchange is no good
    - Eve gets x, y from g^x, g^y and can compute g^{xy} herself

Discrete Log Assumption

- In several groups, PPT adversaries are assumed to have negligible probability of solving the discrete logarithm problem
  - Probability over choice of the group (from a collection), of a generator, and a random group element X
    - DL Expt: $(G,g) \leftarrow \text{GroupGen}$; $X \leftarrow G$; $\text{Adv}(G,g,X) \rightarrow z$; $g^z = X$?
  - If Eve could solve the discrete logarithm (DL) problem, then Diffie-Hellman key-exchange is no good
    - Eve gets x, y from g^x, g^y and can compute g^{xy} herself
      - A "key-recovery" attack

A Candidate DLA Group

A Candidate DLA Group

- The cyclic group $\mathbb{Z}_p^*$ (P prime)

A Candidate DLA Group

- The cyclic group $\mathbb{Z}_p^*$ (P prime)
  - Has N=P-1 elements

A Candidate DLA Group

- The cyclic group $\mathbb{Z}_P^*$ (P prime)
  - Has N=P-1 elements
  - Isomorphic to $\mathbb{Z}_N$ (Isomorphism: discrete log w.r.t a generator. A different isomorphism for each generator)

A Candidate DLA Group

- The cyclic group $\mathbb{Z}_P^*$ (P prime)
  - Has N=P-1 elements
  - Isomorphic to $\mathbb{Z}_N$ (Isomorphism: discrete log w.r.t a generator. A different isomorphism for each generator)

A Candidate DLA Group

- The cyclic group $\mathbb{Z}_P^*$ (P prime)
  - Has N=P-1 elements
  - Isomorphic to $\mathbb{Z}_N$ (Isomorphism: discrete log w.r.t a generator. A different isomorphism for each generator)
  - Discrete Logarithm problem (given "std rep.") considered hard

A Candidate DLA Group

- The cyclic group $\mathbb{Z}_P^*$ (P prime)
  - Has N=P-1 elements
  - Isomorphic to $\mathbb{Z}_N$ (Isomorphism: discrete log w.r.t a generator. A different isomorphism for each generator)
  - Discrete Logarithm problem (given "std rep.") considered hard
    - i.e., the isomorphism from $\mathbb{Z}_P^*$ (in "std rep.") to $\mathbb{Z}_N$ is hard to evaluate

Decisional Diffie-Hellman (DDH) Assumption

Decisional Diffie-Hellman (DDH) Assumption

- Assumption that implies CPA security of El Gamal encryption

Decisional Diffie-Hellman (DDH) Assumption

- Assumption that implies CPA security of El Gamal encryption
- $\{(g^x, g^y, g^{xy})\}_{(G,g)\leftarrow \text{GroupGen}; x,y\leftarrow[|G|]} \approx \{(g^x, g^y, g^r)\}_{(G,g)\leftarrow \text{GroupGen}; x,y,r\leftarrow[|G|]}$

Decisional Diffie-Hellman (DDH) Assumption

- Assumption that implies CPA security of El Gamal encryption
- $\{(g^x, g^y, g^{xy})\}_{(G,g)\leftarrow \text{GroupGen}; x,y\leftarrow[|G|]} \approx \{(g^x, g^y, g^r)\}_{(G,g)\leftarrow \text{GroupGen}; x,y,r\leftarrow[|G|]}$
- At least as strong as DLA

Decisional Diffie-Hellman (DDH) Assumption

- Assumption that implies CPA security of El Gamal encryption
- $\{(g^x, g^y, g^{xy})\}_{(G,g)\leftarrow\text{GroupGen}; x,y\leftarrow[|G|]} \approx \{(g^x, g^y, g^r)\}_{(G,g)\leftarrow\text{GroupGen}; x,y,r\leftarrow[|G|]}$
- At least as strong as DLA
  - If DDH assumption holds, then DLA holds [Exercise]

Decisional Diffie-Hellman (DDH) Assumption

- Assumption that implies CPA security of El Gamal encryption
- $\{(g^x, g^y, g^{xy})\}_{(G,g)\leftarrow\text{GroupGen}; x,y\leftarrow[|G|]} \approx \{(g^x, g^y, g^r)\}_{(G,g)\leftarrow\text{GroupGen}; x,y,r\leftarrow[|G|]}$
- At least as strong as DLA
  - If DDH assumption holds, then DLA holds [Exercise]
- But possible that DLA holds and DDH assumption doesn't

Decisional Diffie-Hellman (DDH) Assumption

- Assumption that implies CPA security of El Gamal encryption
- $\{(g^x, g^y, g^{xy})\}_{(G,g)\leftarrow\text{GroupGen}; x,y\leftarrow[|G|]} \approx \{(g^x, g^y, g^r)\}_{(G,g)\leftarrow\text{GroupGen}; x,y,r\leftarrow[|G|]}$
- At least as strong as DLA
  - If DDH assumption holds, then DLA holds [Exercise]
- But possible that DLA holds and DDH assumption doesn't
  - e.g.: DLA is widely assumed to hold in $\mathbb{Z}_p^*$ (p prime), but DDH assumption doesn't hold there!

A Candidate DDH Group

A Candidate DDH Group

- Quadratic (QR): "even" elements

A Candidate DDH Group

- Quadratic (QR): "even" elements

A Candidate DDH Group

- Quadratic (QR): "even" elements
  - Does not change with the generator (why?)

A Candidate DDH Group

- Quadratic (QR): "even" elements
  - Does not change with the generator (why?)
- Easy to check if an element is a QR or not

A Candidate DDH Group

- Quadratic (QR): "even" elements
  - Does not change with the generator (why?)
- Easy to check if an element is a QR or not
  - Enough to check if raising to N/2 gives 1 (identity element) (Why?)

A Candidate DDH Group

- Quadratic (QR): "even" elements
  - Does not change with the generator (why?)
- Easy to check if an element is a QR or not
  - Enough to check if raising to N/2 gives 1 (identity element) (Why?)
- DDH does not hold in $\mathbb{Z}_p^*$

A Candidate DDH Group

- Quadratic (QR): "even" elements
  - Does not change with the generator (why?)
- Easy to check if an element is a QR or not
  - Enough to check if raising to N/2 gives 1 (identity element) (Why?)
- DDH does not hold in $\mathbb{Z}_p^*$
  - g^{xy} is a QR w/ prob. 3/4; g^z only w/ prob. 1/2.

A Candidate DDH Group

- Quadratic (QR): "even" elements
  - Does not change with the generator (why?)
- Easy to check if an element is a QR or not
  - Enough to check if raising to N/2 gives 1 (identity element) (Why?)
- DDH does not hold in $\mathbb{Z}_p^*$
  - g^{xy} is a QR w/ prob. 3/4; g^z only w/ prob. 1/2.
- How about in a subgroup of $\mathbb{Z}_p^*$ such that all are QRs?

A Candidate DDH Group

A Candidate DDH Group

- $\mathbb{QR}_p^*$: All QRs in $\mathbb{Z}_p^*$

A Candidate DDH Group

- $\mathbb{QR}_p^*$: All QRs in $\mathbb{Z}_p^*$
  - Is a (computational) cyclic group of order (P-1)/2 (Why?)

A Candidate DDH Group

- $\mathbb{QR}_P^*$: All QRs in $\mathbb{Z}_P^*$
  - Is a (computational) cyclic group of order (P-1)/2 (Why?)
  - DDH potentially hard?

A Candidate DDH Group

- $\mathbb{QR}_P^*$: All QRs in $\mathbb{Z}_P^*$
  - Is a (computational) cyclic group of order (P-1)/2 (Why?)
  - DDH potentially hard?
  - Could check if cubic residue!

A Candidate DDH Group

- QR_P^*: All QRs in $\mathbb{Z}_P^*$
  - Is a (computational) cyclic group of order (P-1)/2 (Why?)
  - DDH potentially hard?
  - Could check if cubic residue!
    - But if (P-1) is not divisible by 3, all elements in $\mathbb{Z}_P^*$ are cubic residues! (Why?)

A Candidate DDH Group

- $\mathbb{QR}_P^*$: All QRs in $\mathbb{Z}_P^*$
  - Is a (computational) cyclic group of order (P-1)/2 (Why?)
  - DDH potentially hard?
  - Could check if cubic residue!
    - But if (P-1) is not divisible by 3, all elements in $\mathbb{Z}_P^*$ are cubic residues! (Why?)
  - "Safe" if (P-1)/2 is also prime: P called a safe-prime

A Candidate DDH Group

- $\mathbb{QR}_P^*$: All QRs in $\mathbb{Z}_P^*$
  - Is a (computational) cyclic group of order (P-1)/2 (Why?)
  - DDH potentially hard?
  - Could check if cubic residue!
    - But if (P-1) is not divisible by 3, all elements in $\mathbb{Z}_P^*$ are cubic residues! (Why?)
  - "Safe" if (P-1)/2 is also prime: P called a safe-prime
- DDH Candidate

A Candidate DDH Group

- $\mathbb{QR}_P^*$: All QRs in $\mathbb{Z}_P^*$
  - Is a (computational) cyclic group of order (P-1)/2 (Why?)
  - DDH potentially hard?
  - Could check if cubic residue!
    - But if (P-1) is not divisible by 3, all elements in $\mathbb{Z}_P^*$ are cubic residues! (Why?)
  - "Safe" if (P-1)/2 is also prime: P called a safe-prime
- DDH Candidate
  - $\mathbb{QR}_P^*$ where P is a "safe prime"

Towards Trapdoor OWP

Towards Trapdoor OWP

- Two candidates: RSA function and Rabin function

Towards Trapdoor OWP

- Two candidates: RSA function and Rabin function
  - Over appropriate domains

Towards Trapdoor OWP

- Two candidates: RSA function and Rabin function
  - Over appropriate domains
- Will rely on factorization as the trapdoor

Towards Trapdoor OWP

- Two candidates: RSA function and Rabin function
  - Over appropriate domains
- Will rely on factorization as the trapdoor
  - Hence one-wayness will rely on hardness of factoring (and more)

$\mathbb{Z}_N^*$

Extended Euclidean algorithm to find (b,d) given (a,N). Used to efficiently invert elements in $\mathbb{Z}_N^*$

$\mathbb{Z}_N^*$

- Group operation: "multiplication modulo N"

Extended Euclidean algorithm to find (b,d) given (a,N). Used to efficiently invert elements in $\mathbb{Z}_N^*$

$\mathbb{Z}_N^*$

- Group operation: "multiplication modulo N"
  - Has identity, is associative

Extended Euclidean algorithm to find (b,d) given (a,N). Used to efficiently invert elements in $\mathbb{Z}_N^*$

$\mathbb{Z}_N^*$

- Group operation: "multiplication modulo N"
  - Has identity, is associative
- Group elements: all numbers (mod N) which have a multiplicative inverse modulo N

Extended Euclidean algorithm to find (b,d) given (a,N). Used to efficiently invert elements in $\mathbb{Z}_N^*$

$\mathbb{Z}_N^*$

- Group operation: "multiplication modulo N"
  - Has identity, is associative
- Group elements: all numbers (mod N) which have a multiplicative inverse modulo N
  - e.g.: $\mathbb{Z}_6^*$ has elements {1,5}, $\mathbb{Z}_7^*$ has {1,2,3,4,5,6}

Extended Euclidean algorithm to find (b,d) given (a,N). Used to efficiently invert elements in $\mathbb{Z}_N^*$

$\mathbb{Z}_N^*$

- Group operation: "multiplication modulo N"
  - Has identity, is associative
- Group elements: all numbers (mod N) which have a multiplicative inverse modulo N
  - e.g.: $\mathbb{Z}_6^*$ has elements {1,5}, $\mathbb{Z}_7^*$ has {1,2,3,4,5,6}
- a has a multiplicative inverse modulo N

Extended Euclidean algorithm to find (b,d) given (a,N). Used to efficiently invert elements in $\mathbb{Z}_N^*$

$\mathbb{Z}_N^*$

- Group operation: "multiplication modulo N"
  - Has identity, is associative
- Group elements: all numbers (mod N) which have a multiplicative inverse modulo N
  - e.g.: $\mathbb{Z}_6^*$ has elements {1,5}, $\mathbb{Z}_7^*$ has {1,2,3,4,5,6}
- a has a multiplicative inverse modulo N
  - $\Leftrightarrow \exists$ integers b, c s.t. $ab = 1+cN$

Extended Euclidean algorithm to find (b,d) given (a,N). Used to efficiently invert elements in $\mathbb{Z}_N^*$

$\mathbb{Z}_N^*$

- Group operation: "multiplication modulo N"
  - Has identity, is associative
- Group elements: all numbers (mod N) which have a multiplicative inverse modulo N
  - e.g.: $\mathbb{Z}_6^*$ has elements {1,5}, $\mathbb{Z}_7^*$ has {1,2,3,4,5,6}
- a has a multiplicative inverse modulo N
  - $\Leftrightarrow \exists$ integers b, c s.t. ab = 1+cN
  - $\Leftrightarrow$ gcd(a,N)=1

Extended Euclidean algorithm to find (b,d) given (a,N). Used to efficiently invert elements in $\mathbb{Z}_N^*$

$\mathbb{Z}_N^*$

- Group operation: "multiplication modulo N"
  - Has identity, is associative
- Group elements: all numbers (mod N) which have a multiplicative inverse modulo N
  - e.g.: $\mathbb{Z}_6^*$ has elements {1,5}, $\mathbb{Z}_7^*$ has {1,2,3,4,5,6}
- a has a multiplicative inverse modulo N
  - $\Leftrightarrow$ $\exists$ integers b, c s.t. ab = 1+cN
  - $\Leftrightarrow$ gcd(a,N)=1
    - ($\Rightarrow$) gcd(a,N) | (ab-cN)

Extended Euclidean algorithm to find (b,d) given (a,N). Used to efficiently invert elements in $\mathbb{Z}_N^*$

$\mathbb{Z}_N^*$

- Group operation: "multiplication modulo N"
  - Has identity, is associative
- Group elements: all numbers (mod N) which have a multiplicative inverse modulo N
  - e.g.: $\mathbb{Z}_6^*$ has elements {1,5}, $\mathbb{Z}_7^*$ has {1,2,3,4,5,6}
- a has a multiplicative inverse modulo N
  - $\Leftrightarrow$ $\exists$ integers b, c s.t. ab = 1+cN
  - $\Leftrightarrow$ gcd(a,N)=1
    - ($\Rightarrow$) gcd(a,N) | (ab-cN)
    - ($\Leftarrow$) from Euclid's algorithm: $\exists$ b, d s.t. gcd(a,N) = ab+dN

Extended Euclidean algorithm to find (b,d) given (a,N). Used to efficiently invert elements in $\mathbb{Z}_N^*$

$\mathbb{Z}_N^*$

- Group operation: "multiplication modulo N"
  - Has identity, is associative
- Group elements: all numbers (mod N) which have a multiplicative inverse modulo N
  - e.g.: $\mathbb{Z}_6^*$ has elements {1,5}, $\mathbb{Z}_7^*$ has {1,2,3,4,5,6}
- a has a multiplicative inverse modulo N
  - $\Leftrightarrow \exists$ integers b, c s.t. ab = 1+cN
  - $\Leftrightarrow$ gcd(a,N)=1
    - ($\Rightarrow$) gcd(a,N) | (ab-cN)
    - ($\Leftarrow$) from Euclid's algorithm: $\exists$ b, d s.t. gcd(a,N) = ab+dN
  - $|\mathbb{Z}_N^*|$ = #integers in [1,N-1] co-prime with N = $\varphi(N)$

Extended Euclidean algorithm to find (b,d) given (a,N). Used to efficiently invert elements in $\mathbb{Z}_N^*$

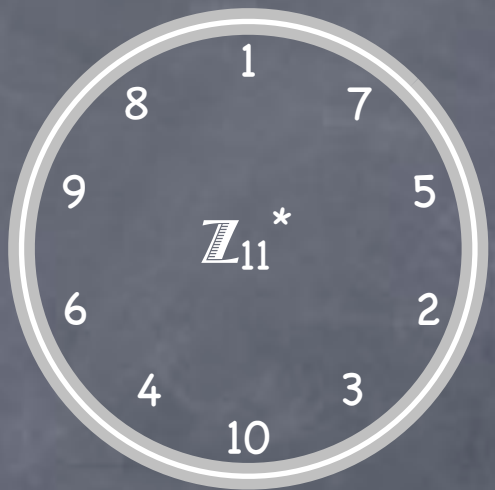
$\mathbb{Z}_p^*$, p prime

$\mathbb{Z}_p^*$, p prime

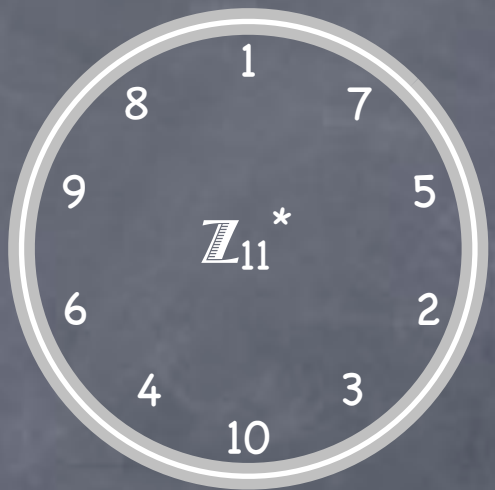
- Recall $\mathbb{Z}_p^*$

$\mathbb{Z}_p^*$, p prime

- Recall $\mathbb{Z}_p^*$

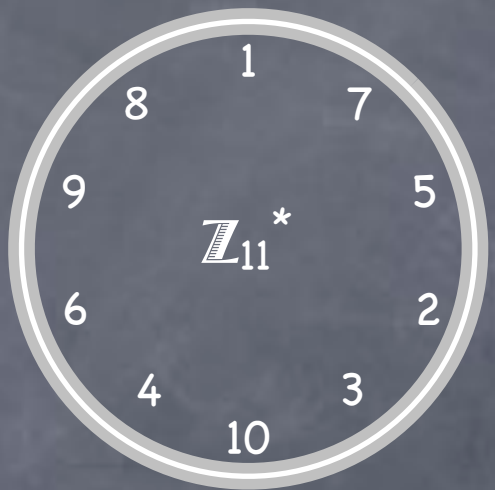


$\mathbb{Z}_p^*$, P prime



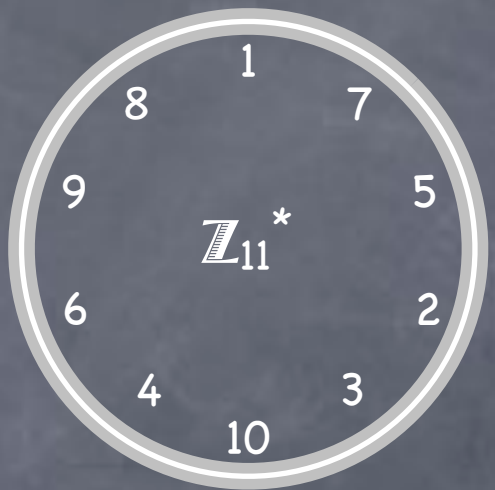
- Recall $\mathbb{Z}_p^*$
- $|\mathbb{Z}_p^*| = P-1$ (all of them co-prime with P)

$\mathbb{Z}_p^*$, p prime



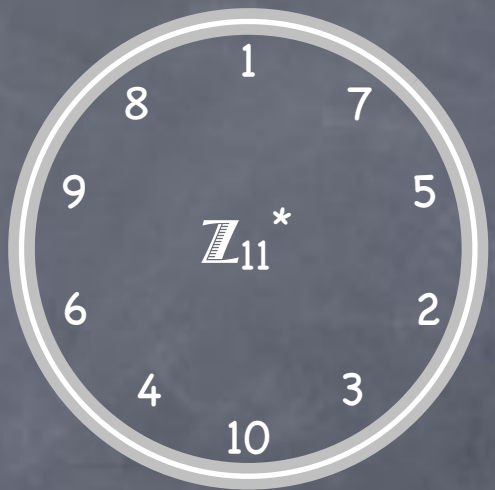
- Recall $\mathbb{Z}_p^*$
- $|\mathbb{Z}_p^*| = p-1$ (all of them co-prime with p)
- Cyclic: Isomorphic to $\mathbb{Z}_{p-1}$

$\mathbb{Z}_p^*$, P prime



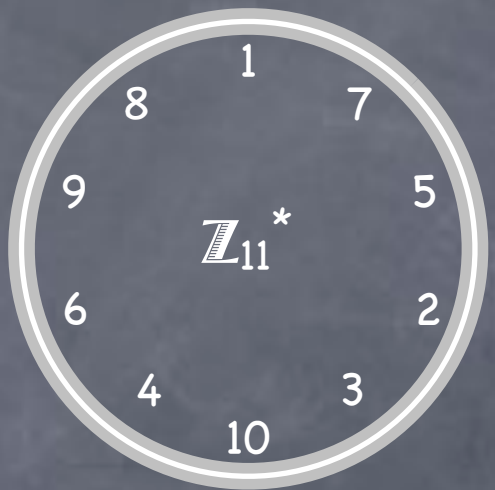
- Recall $\mathbb{Z}_p^*$
- $|\mathbb{Z}_p^*| = P-1$ (all of them co-prime with P)
- Cyclic: Isomorphic to $\mathbb{Z}_{P-1}$
  - Has $\varphi(P-1)$ different generators

$\mathbb{Z}_P^*$, P prime



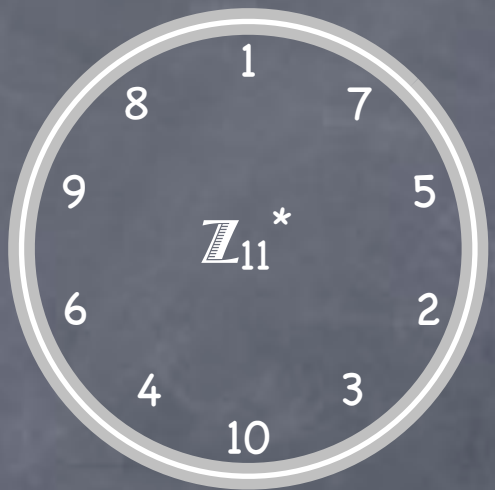
- Recall $\mathbb{Z}_P^*$
- $|\mathbb{Z}_P^*| = P-1$ (all of them co-prime with P)
- Cyclic: Isomorphic to $\mathbb{Z}_{P-1}$
  - Has $\varphi(P-1)$ different generators
- Discrete Log assumed to be hard

$\mathbb{Z}_p^*$, p prime



- Recall $\mathbb{Z}_p^*$
- $|\mathbb{Z}_p^*| = p-1$ (all of them co-prime with p)
- Cyclic: Isomorphic to $\mathbb{Z}_{p-1}$
  - Has $\varphi(p-1)$ different generators
- Discrete Log assumed to be hard
- Quadratic Residues form a subgroup $\mathbb{QR}_p^*$

$\mathbb{Z}_p^*$, P prime



- Recall $\mathbb{Z}_p^*$
- $|\mathbb{Z}_p^*| = P-1$ (all of them co-prime with P)
- Cyclic: Isomorphic to $\mathbb{Z}_{P-1}$
  - Has $\varphi(P-1)$ different generators
- Discrete Log assumed to be hard
- Quadratic Residues form a subgroup $\mathbb{QR}_p^*$
  - Candidate group for DDH assumption

$\mathbb{Z}_N^*$, N=PQ, two primes

$\mathbb{Z}_N^*$, N=PQ, two primes

- e.g. $\mathbb{Z}_{15}^* = \{1,2,4,7,8,11,13,14\}$

$\mathbb{Z}_N^*$, N=PQ, two primes

- e.g. $\mathbb{Z}_{15}^* = \{1,2,4,7,8,11,13,14\}$
- $|\mathbb{Z}_{PQ}^*| = (P-1)(Q-1)$ ($P \neq Q$, primes)

$\mathbb{Z}_N^*$, N=PQ, two primes

- e.g. $\mathbb{Z}_{15}^* = \{1,2,4,7,8,11,13,14\}$
- $|\mathbb{Z}_{PQ}^*| = (P-1)(Q-1)$ ($P \neq Q$, primes)
- Cyclic?

$\mathbb{Z}_N^*$, N=PQ, two primes

- e.g. $\mathbb{Z}_{15}^* = \{1,2,4,7,8,11,13,14\}$
- $|\mathbb{Z}_{PQ}^*| = (P-1)(Q-1)$ ($P \neq Q$, primes)
- Cyclic?
  - No! In $\mathbb{Z}_{15}^*$, $2^4 = 4^2 = 7^4 = 8^4 = 11^2 = 13^4 = 14^2 = 1$
    (i.e., each generates at most 4 elements, out of 8)

$\mathbb{Z}_N^*$, N=PQ, two primes

- e.g. $\mathbb{Z}_{15}^* = \{1,2,4,7,8,11,13,14\}$
- $|\mathbb{Z}_{PQ}^*| = (P-1)(Q-1)$ ($P \neq Q$, primes)
- Cyclic?
  - No! In $\mathbb{Z}_{15}^*$, $2^4 = 4^2 = 7^4 = 8^4 = 11^2 = 13^4 = 14^2 = 1$
    (i.e., each generates at most 4 elements, out of 8)
- "Product of two cycles": $\mathbb{Z}_3^*$ and $\mathbb{Z}_5^*$

$\mathbb{Z}_N^*$, N=PQ, two primes

- e.g. $\mathbb{Z}_{15}^* = \{1,2,4,7,8,11,13,14\}$
- $|\mathbb{Z}_{PQ}^*| = (P-1)(Q-1)$ ($P \neq Q$, primes)
- Cyclic?
  - No! In $\mathbb{Z}_{15}^*$, $2^4 = 4^2 = 7^4 = 8^4 = 11^2 = 13^4 = 14^2 = 1$
    (i.e., each generates at most 4 elements, out of 8)
- "Product of two cycles": $\mathbb{Z}_3^*$ and $\mathbb{Z}_5^*$
  - Chinese Remainder Theorem

Chinese Remainder Theorem

Chinese Remainder Theorem

- Consider mapping elements in $\mathbb{Z}_{15}$ (all 15 of them) to $\mathbb{Z}_3$ and $\mathbb{Z}_5$

Chinese Remainder Theorem

- Consider mapping elements in $\mathbb{Z}_{15}$ (all 15 of them) to $\mathbb{Z}_3$ and $\mathbb{Z}_5$
  - $a \mapsto (a \bmod 3, a \bmod 5)$

Chinese Remainder Theorem

$\mathbb{Z}_{15}$	$\mathbb{Z}_3$	$\mathbb{Z}_5$

- Consider mapping elements in $\mathbb{Z}_{15}$ (all 15 of them) to $\mathbb{Z}_3$ and $\mathbb{Z}_5$
  - $a \mapsto (a \bmod 3, a \bmod 5)$

Chinese Remainder Theorem

$\mathbb{Z}_{15}$	$\mathbb{Z}_3$	$\mathbb{Z}_5$
0	0	0

- Consider mapping elements in $\mathbb{Z}_{15}$ (all 15 of them) to $\mathbb{Z}_3$ and $\mathbb{Z}_5$
  - $a \mapsto (a \bmod 3, a \bmod 5)$

Chinese Remainder Theorem

$\mathbb{Z}_{15}$	$\mathbb{Z}_3$	$\mathbb{Z}_5$
0	0	0
1	1	1

- Consider mapping elements in $\mathbb{Z}_{15}$ (all 15 of them) to $\mathbb{Z}_3$ and $\mathbb{Z}_5$
  - $a \mapsto (a \bmod 3, a \bmod 5)$

Chinese Remainder Theorem

- Consider mapping elements in $\mathbb{Z}_{15}$ (all 15 of them) to $\mathbb{Z}_3$ and $\mathbb{Z}_5$
  - $a \mapsto (a \bmod 3, a \bmod 5)$

$\mathbb{Z}_{15}$	$\mathbb{Z}_3$	$\mathbb{Z}_5$
0	0	0
1	1	1
2	2	2

Chinese Remainder Theorem

- Consider mapping elements in $\mathbb{Z}_{15}$ (all 15 of them) to $\mathbb{Z}_3$ and $\mathbb{Z}_5$
  - $a \mapsto (a \bmod 3, a \bmod 5)$

$\mathbb{Z}_{15}$	$\mathbb{Z}_3$	$\mathbb{Z}_5$
0	0	0
1	1	1
2	2	2
3	0	3
4	1	4
5	2	0
6	0	1
7	1	2
8	2	3
9	0	4
10	1	0
11	2	1
12	0	2
13	1	3
14	2	4

Chinese Remainder Theorem

- Consider mapping elements in $\mathbb{Z}_{15}$ (all 15 of them) to $\mathbb{Z}_3$ and $\mathbb{Z}_5$
  - $a \mapsto (a \bmod 3, a \bmod 5)$
- CRT says that the pair $(a \bmod 3, a \bmod 5)$ uniquely determines $a \pmod{15}$!

$\mathbb{Z}_{15}$	$\mathbb{Z}_3$	$\mathbb{Z}_5$
0	0	0
1	1	1
2	2	2
3	0	3
4	1	4
5	2	0
6	0	1
7	1	2
8	2	3
9	0	4
10	1	0
11	2	1
12	0	2
13	1	3
14	2	4

Chinese Remainder Theorem

- Consider mapping elements in $\mathbb{Z}_{15}$ (all 15 of them) to $\mathbb{Z}_3$ and $\mathbb{Z}_5$
  - $a \mapsto (a \bmod 3, a \bmod 5)$
- CRT says that the pair (a mod 3, a mod 5) uniquely determines a (mod 15)!
  - All 15 possible pairs occur, once each

$\mathbb{Z}_{15}$	$\mathbb{Z}_3$	$\mathbb{Z}_5$
0	0	0
1	1	1
2	2	2
3	0	3
4	1	4
5	2	0
6	0	1
7	1	2
8	2	3
9	0	4
10	1	0
11	2	1
12	0	2
13	1	3
14	2	4

Chinese Remainder Theorem

- Consider mapping elements in $\mathbb{Z}_{15}$ (all 15 of them) to $\mathbb{Z}_3$ and $\mathbb{Z}_5$
  - $a \mapsto (a \bmod 3, a \bmod 5)$
- CRT says that the pair (a mod 3, a mod 5) uniquely determines a (mod 15)!
  - All 15 possible pairs occur, once each
- In general for N=PQ (P, Q relatively prime), $a \mapsto (a \bmod P, a \bmod Q)$ maps the N elements to the N distinct pairs

$\mathbb{Z}_{15}$	$\mathbb{Z}_3$	$\mathbb{Z}_5$
0	0	0
1	1	1
2	2	2
3	0	3
4	1	4
5	2	0
6	0	1
7	1	2
8	2	3
9	0	4
10	1	0
11	2	1
12	0	2
13	1	3
14	2	4

Chinese Remainder Theorem

- Consider mapping elements in $\mathbb{Z}_{15}$ (all 15 of them) to $\mathbb{Z}_3$ and $\mathbb{Z}_5$
  - $a \mapsto (a \bmod 3, a \bmod 5)$
- CRT says that the pair (a mod 3, a mod 5) uniquely determines a (mod 15)!
  - All 15 possible pairs occur, once each
- In general for N=PQ (P, Q relatively prime), $a \mapsto (a \bmod P, a \bmod Q)$ maps the N elements to the N distinct pairs
  - In fact extends to product of more than two (relatively prime) numbers

$\mathbb{Z}_{15}$	$\mathbb{Z}_3$	$\mathbb{Z}_5$
0	0	0
1	1	1
2	2	2
3	0	3
4	1	4
5	2	0
6	0	1
7	1	2
8	2	3
9	0	4
10	1	0
11	2	1
12	0	2
13	1	3
14	2	4

Chinese Remainder Theorem and $\mathbb{Z}_N$

$\mathbb{Z}_{15}$	$\mathbb{Z}_3$	$\mathbb{Z}_5$
0	0	0
1	1	1
2	2	2
3	0	3
4	1	4
5	2	0
6	0	1
7	1	2
8	2	3
9	0	4
10	1	0
11	2	1
12	0	2
13	1	3
14	2	4

Chinese Remainder Theorem and $\mathbb{Z}_N$

- CRT representation of $\mathbb{Z}_N$: every element of $\mathbb{Z}_N$ can be written as a unique element of $\mathbb{Z}_P \times \mathbb{Z}_Q$

$\mathbb{Z}_{15}$	$\mathbb{Z}_3$	$\mathbb{Z}_5$
0	0	0
1	1	1
2	2	2
3	0	3
4	1	4
5	2	0
6	0	1
7	1	2
8	2	3
9	0	4
10	1	0
11	2	1
12	0	2
13	1	3
14	2	4

Chinese Remainder Theorem and $\mathbb{Z}_N$

- CRT representation of $\mathbb{Z}_N$: every element of $\mathbb{Z}_N$ can be written as a unique element of $\mathbb{Z}_P \times \mathbb{Z}_Q$
  - Addition can be done coordinate-wise

$\mathbb{Z}_{15}$	$\mathbb{Z}_3$	$\mathbb{Z}_5$
0	0	0
1	1	1
2	2	2
3	0	3
4	1	4
5	2	0
6	0	1
7	1	2
8	2	3
9	0	4
10	1	0
11	2	1
12	0	2
13	1	3
14	2	4

Chinese Remainder Theorem and $\mathbb{Z}_N$

- CRT representation of $\mathbb{Z}_N$: every element of $\mathbb{Z}_N$ can be written as a unique element of $\mathbb{Z}_P \times \mathbb{Z}_Q$
  - Addition can be done coordinate-wise
  - $(a,b) +_{(\text{mod } N)} (a',b') = (a +_{(\text{mod } P)} a', b +_{(\text{mod } Q)} b')$

$\mathbb{Z}_{15}$	$\mathbb{Z}_3$	$\mathbb{Z}_5$
0	0	0
1	1	1
2	2	2
3	0	3
4	1	4
5	2	0
6	0	1
7	1	2
8	2	3
9	0	4
10	1	0
11	2	1
12	0	2
13	1	3
14	2	4

Chinese Remainder Theorem and $\mathbb{Z}_N$

- CRT representation of $\mathbb{Z}_N$: every element of $\mathbb{Z}_N$ can be written as a unique element of $\mathbb{Z}_P \times \mathbb{Z}_Q$
  - Addition can be done coordinate-wise
  - $(a,b) +_{(\text{mod } N)} (a',b') = (a +_{(\text{mod } P)} a', b +_{(\text{mod } Q)} b')$
- CRT: $\mathbb{Z}_N \cong \mathbb{Z}_P \times \mathbb{Z}_Q$ (group isomorphism)

$\mathbb{Z}_{15}$	$\mathbb{Z}_3$	$\mathbb{Z}_5$
0	0	0
1	1	1
2	2	2
3	0	3
4	1	4
5	2	0
6	0	1
7	1	2
8	2	3
9	0	4
10	1	0
11	2	1
12	0	2
13	1	3
14	2	4

Chinese Remainder Theorem and $\mathbb{Z}_N^*$

$\mathbb{Z}_{15}$	$\mathbb{Z}_3$	$\mathbb{Z}_5$
0	0	0
1	1	1
2	2	2
3	0	3
4	1	4
5	2	0
6	0	1
7	1	2
8	2	3
9	0	4
10	1	0
11	2	1
12	0	2
13	1	3
14	2	4

Chinese Remainder Theorem and $\mathbb{Z}_N^*$

- Elements in $\mathbb{Z}_N^*$

$\mathbb{Z}_{15}$	$\mathbb{Z}_3$	$\mathbb{Z}_5$
0	0	0
1	1	1
2	2	2
3	0	3
4	1	4
5	2	0
6	0	1
7	1	2
8	2	3
9	0	4
10	1	0
11	2	1
12	0	2
13	1	3
14	2	4

Chinese Remainder Theorem and $\mathbb{Z}_N^*$

- Elements in $\mathbb{Z}_N^*$
  - No multiplicative inverse iff (0,x) or (x,0)

$\mathbb{Z}_{15}$	$\mathbb{Z}_3$	$\mathbb{Z}_5$
0	0	0
1	1	1
2	2	2
3	0	3
4	1	4
5	2	0
6	0	1
7	1	2
8	2	3
9	0	4
10	1	0
11	2	1
12	0	2
13	1	3
14	2	4

Chinese Remainder Theorem and $\mathbb{Z}_N^*$

- Elements in $\mathbb{Z}_N^*$
  - No multiplicative inverse iff (0,x) or (x,0)
    - Multiplication (and identity, inverse) also coordinate-wise

$\mathbb{Z}_{15}$	$\mathbb{Z}_3$	$\mathbb{Z}_5$
0	0	0
1	1	1
2	2	2
3	0	3
4	1	4
5	2	0
6	0	1
7	1	2
8	2	3
9	0	4
10	1	0
11	2	1
12	0	2
13	1	3
14	2	4

Chinese Remainder Theorem and $\mathbb{Z}_N^*$

- Elements in $\mathbb{Z}_N^*$
  - No multiplicative inverse iff (0,x) or (x,0)
    - Multiplication (and identity, inverse) also coordinate-wise
  - Else in $\mathbb{Z}_N^*$: i.e., (x,y) s.t. $x \in \mathbb{Z}_P^*$, $y \in \mathbb{Z}_Q^*$

$\mathbb{Z}_{15}$	$\mathbb{Z}_3$	$\mathbb{Z}_5$
0	0	0
1	1	1
2	2	2
3	0	3
4	1	4
5	2	0
6	0	1
7	1	2
8	2	3
9	0	4
10	1	0
11	2	1
12	0	2
13	1	3
14	2	4

Chinese Remainder Theorem and $\mathbb{Z}_N^*$

- Elements in $\mathbb{Z}_N^*$
  - No multiplicative inverse iff (0,x) or (x,0)
    - Multiplication (and identity, inverse) also coordinate-wise
  - Else in $\mathbb{Z}_N^*$: i.e., (x,y) s.t. $x \in \mathbb{Z}_P^*$, $y \in \mathbb{Z}_Q^*$
    - $\mathbb{Z}_N^* \cong \mathbb{Z}_P^* \times \mathbb{Z}_Q^*$

$\mathbb{Z}_{15}$	$\mathbb{Z}_3$	$\mathbb{Z}_5$
0	0	0
1	1	1
2	2	2
3	0	3
4	1	4
5	2	0
6	0	1
7	1	2
8	2	3
9	0	4
10	1	0
11	2	1
12	0	2
13	1	3
14	2	4

Chinese Remainder Theorem and $\mathbb{Z}_N^*$

- Elements in $\mathbb{Z}_N^*$
  - No multiplicative inverse iff (0,x) or (x,0)
    - Multiplication (and identity, inverse) also coordinate-wise
  - Else in $\mathbb{Z}_N^*$: i.e., (x,y) s.t. $x \in \mathbb{Z}_P^*$, $y \in \mathbb{Z}_Q^*$
    - $\mathbb{Z}_N^* \cong \mathbb{Z}_P^* \times \mathbb{Z}_Q^*$
- Easy to compute the isomorphism (in both directions) if P, Q known [Exercise]

$\mathbb{Z}_{15}$	$\mathbb{Z}_3$	$\mathbb{Z}_5$
0	0	0
1	1	1
2	2	2
3	0	3
4	1	4
5	2	0
6	0	1
7	1	2
8	2	3
9	0	4
10	1	0
11	2	1
12	0	2
13	1	3
14	2	4

RSA Function

RSA Function

- $f_{RSA[N,e]}(x) = x^e \bmod N$

RSA Function

- $f_{RSA[N,e]}(x) = x^e \bmod N$
  - Where $N=PQ$, and $\gcd(e,\varphi(N)) = 1$

RSA Function

- $f_{RSA[N,e]}(x) = x^e \bmod N$
  - Where $N=PQ$, and $\gcd(e,\varphi(N)) = 1$
  - $f_{RSA[N,e]}: \mathbb{Z}_N \rightarrow \mathbb{Z}_N$

RSA Function

- $f_{RSA[N,e]}(x) = x^e \bmod N$
  - Where $N=PQ$, and $\gcd(e,\varphi(N)) = 1$
  - $f_{RSA[N,e]}: \mathbb{Z}_N \rightarrow \mathbb{Z}_N$
    - Alternately, $f_{RSA[N,e]}: \mathbb{Z}_N^* \rightarrow \mathbb{Z}_N^*$

RSA Function

- $f_{RSA[N,e]}(x) = x^e \bmod N$
  - Where $N=PQ$, and $\gcd(e,\varphi(N)) = 1$
  - $f_{RSA[N,e]}: \mathbb{Z}_N \rightarrow \mathbb{Z}_N$
    - Alternately, $f_{RSA[N,e]}: \mathbb{Z}_N^* \rightarrow \mathbb{Z}_N^*$
- $f_{RSA[N,e]}$ is a permutation

RSA Function

- $f_{RSA[N,e]}(x) = x^e \bmod N$
  - Where N=PQ, and $\gcd(e,\varphi(N)) = 1$
  - $f_{RSA[N,e]}: \mathbb{Z}_N \rightarrow \mathbb{Z}_N$
    - Alternately, $f_{RSA[N,e]}: \mathbb{Z}_N^* \rightarrow \mathbb{Z}_N^*$
- $f_{RSA[N,e]}$ is a permutation
  - In fact, there exists d s.t. $f_{RSA[N,d]}$ is the inverse of $f_{RSA[N,e]}$

RSA Function

- $f_{RSA[N,e]}(x) = x^e \bmod N$
  - Where $N=PQ$, and $\gcd(e,\varphi(N)) = 1$
  - $f_{RSA[N,e]}: \mathbb{Z}_N \rightarrow \mathbb{Z}_N$
    - Alternately, $f_{RSA[N,e]}: \mathbb{Z}_N^* \rightarrow \mathbb{Z}_N^*$
- $f_{RSA[N,e]}$ is a permutation
  - In fact, there exists d s.t. $f_{RSA[N,d]}$ is the inverse of $f_{RSA[N,e]}$
    - d s.t. $ed=1 \pmod{\varphi(N)}$, $x^{ed} = x \pmod N$

RSA Function

- $f_{RSA[N,e]}(x) = x^e \bmod N$
  - Where $N=PQ$, and $\gcd(e,\varphi(N)) = 1$
  - $f_{RSA[N,e]}: \mathbb{Z}_N \rightarrow \mathbb{Z}_N$
    - Alternately, $f_{RSA[N,e]}: \mathbb{Z}_N^* \rightarrow \mathbb{Z}_N^*$
- $f_{RSA[N,e]}$ is a permutation
  - In fact, there exists d s.t. $f_{RSA[N,d]}$ is the inverse of $f_{RSA[N,e]}$
    - d s.t. $ed=1 \pmod{\varphi(N)}$, $x^{ed} = x \pmod N$
    - For $\mathbb{Z}_N^*$ because order is $\varphi(N)$

RSA Function

- $f_{RSA[N,e]}(x) = x^e \bmod N$
  - Where $N=PQ$, and $\gcd(e,\varphi(N)) = 1$
  - $f_{RSA[N,e]}: \mathbb{Z}_N \to \mathbb{Z}_N$
    - Alternately, $f_{RSA[N,e]}: \mathbb{Z}_N^* \to \mathbb{Z}_N^*$
- $f_{RSA[N,e]}$ is a permutation
  - In fact, there exists d s.t. $f_{RSA[N,d]}$ is the inverse of $f_{RSA[N,e]}$
    - d s.t. $ed=1 \pmod{\varphi(N)}$, $x^{ed} = x \pmod N$
    - For $\mathbb{Z}_N^*$ because order is $\varphi(N)$
    - For $\mathbb{Z}_N$? By CRT, and because multiplication is coordinate-wise (and it holds in $\mathbb{Z}_P$ and $\mathbb{Z}_Q$. note: $0^{ed} = 0$) [Exercise]

RSA Function

- $f_{RSA[N,e]}(x) = x^e \bmod N$
  - Where $N=PQ$, and $\gcd(e,\varphi(N)) = 1$
  - $f_{RSA[N,e]}: \mathbb{Z}_N \to \mathbb{Z}_N$
    - Alternately, $f_{RSA[N,e]}: \mathbb{Z}_N^* \to \mathbb{Z}_N^*$
- $f_{RSA[N,e]}$ is a permutation with a trapdoor (namely (N,d))
  - In fact, there exists d s.t. $f_{RSA[N,d]}$ is the inverse of $f_{RSA[N,e]}$
    - d s.t. $ed=1 \pmod{\varphi(N)}$, $x^{ed} = x \pmod N$
    - For $\mathbb{Z}_N^*$ because order is $\varphi(N)$
    - For $\mathbb{Z}_N$? By CRT, and because multiplication is coordinate-wise (and it holds in $\mathbb{Z}_P$ and $\mathbb{Z}_Q$. note: $0^{ed} = 0$) [Exercise]

RSA Function

- $f_{RSA[N,e]}(x) = x^e \bmod N$
  - Where N=PQ, and $\gcd(e,\varphi(N)) = 1$
  - $f_{RSA[N,e]}: \mathbb{Z}_N \rightarrow \mathbb{Z}_N$
    - Alternately, $f_{RSA[N,e]}: \mathbb{Z}_N^* \rightarrow \mathbb{Z}_N^*$
- $f_{RSA[N,e]}$ is a permutation with a trapdoor (namely (N,d))

RSA Function

- $f_{RSA[N,e]}(x) = x^e \bmod N$
  - Where $N=PQ$, and $\gcd(e,\varphi(N)) = 1$
  - $f_{RSA[N,e]}: \mathbb{Z}_N \rightarrow \mathbb{Z}_N$
    - Alternately, $f_{RSA[N,e]}: \mathbb{Z}_N^* \rightarrow \mathbb{Z}_N^*$
- $f_{RSA[N,e]}$ is a permutation with a trapdoor (namely (N,d))
- RSA Assumption: $f_{RSA[N,e]}$ is a OWF collection, when P, Q random k-bit primes and $e < N$ random number s.t. $\gcd(e,\varphi(N))=1$ (with inputs uniformly from $\mathbb{Z}_N$ or $\mathbb{Z}_N^*$)

RSA Function

- $f_{RSA[N,e]}(x) = x^e \bmod N$
  - Where $N=PQ$, and $\gcd(e,\varphi(N)) = 1$
  - $f_{RSA[N,e]}: \mathbb{Z}_N \rightarrow \mathbb{Z}_N$
    - Alternately, $f_{RSA[N,e]}: \mathbb{Z}_N^* \rightarrow \mathbb{Z}_N^*$
- $f_{RSA[N,e]}$ is a permutation with a trapdoor (namely (N,d))
- RSA Assumption: $f_{RSA[N,e]}$ is a OWF collection, when P, Q random k-bit primes and $e < N$ random number s.t. $\gcd(e,\varphi(N))=1$ (with inputs uniformly from $\mathbb{Z}_N$ or $\mathbb{Z}_N^*$)
  - Alternate version: $e=3$, P, Q restricted so that $\gcd(3,\varphi(N))=1$

RSA Function

- $f_{RSA[N,e]}(x) = x^e \bmod N$
  - Where N=PQ, and $\gcd(e,\varphi(N)) = 1$
  - $f_{RSA[N,e]}: \mathbb{Z}_N \rightarrow \mathbb{Z}_N$
    - Alternately, $f_{RSA[N,e]}: \mathbb{Z}_N^* \rightarrow \mathbb{Z}_N^*$
- $f_{RSA[N,e]}$ is a permutation with a trapdoor (namely (N,d))
- RSA Assumption: $f_{RSA[N,e]}$ is a OWF collection, when P, Q random k-bit primes and e < N random number s.t. $\gcd(e,\varphi(N))=1$ (with inputs uniformly from $\mathbb{Z}_N$ or $\mathbb{Z}_N^*$)
  - Alternate version: e=3, P, Q restricted so that $\gcd(3,\varphi(N))=1$
- RSA Assumption will be false if one can factorize N

RSA Function

- $f_{RSA[N,e]}(x) = x^e \bmod N$
  - Where N=PQ, and gcd(e,φ(N)) = 1
  - $f_{RSA[N,e]}: \mathbb{Z}_N \rightarrow \mathbb{Z}_N$
    - Alternately, $f_{RSA[N,e]}: \mathbb{Z}_N^* \rightarrow \mathbb{Z}_N^*$
- $f_{RSA[N,e]}$ is a permutation with a trapdoor (namely (N,d))
- RSA Assumption: $f_{RSA[N,e]}$ is a OWF collection, when P, Q random k-bit primes and e < N random number s.t. gcd(e,φ(N))=1 (with inputs uniformly from $\mathbb{Z}_N$ or $\mathbb{Z}_N^*$)
  - Alternate version: e=3, P, Q restricted so that gcd(3,φ(N))=1
- RSA Assumption will be false if one can factorize N
  - Then knows φ(N) and can find $d=e^{-1}$ in $\mathbb{Z}_{\varphi(N)}^*$

RSA Function

- $f_{RSA[N,e]}(x) = x^e \bmod N$
  - Where N=PQ, and gcd(e,φ(N)) = 1
  - $f_{RSA[N,e]}: \mathbb{Z}_N \rightarrow \mathbb{Z}_N$
    - Alternately, $f_{RSA[N,e]}: \mathbb{Z}_N^* \rightarrow \mathbb{Z}_N^*$
- $f_{RSA[N,e]}$ is a permutation with a trapdoor (namely (N,d))
- RSA Assumption: $f_{RSA[N,e]}$ is a OWF collection, when P, Q random k-bit primes and e < N random number s.t. gcd(e,φ(N))=1 (with inputs uniformly from $\mathbb{Z}_N$ or $\mathbb{Z}_N^*$)
  - Alternate version: e=3, P, Q restricted so that gcd(3,φ(N))=1
- RSA Assumption will be false if one can factorize N
  - Then knows φ(N) and can find $d=e^{-1}$ in $\mathbb{Z}_{\varphi(N)}^*$
  - Converse not known to hold

RSA Function

- $f_{RSA[N,e]}(x) = x^e \bmod N$
  - Where $N=PQ$, and $\gcd(e,\varphi(N)) = 1$
  - $f_{RSA[N,e]}: \mathbb{Z}_N \rightarrow \mathbb{Z}_N$
    - Alternately, $f_{RSA[N,e]}: \mathbb{Z}_N^* \rightarrow \mathbb{Z}_N^*$
- $f_{RSA[N,e]}$ is a permutation with a trapdoor (namely (N,d))
- RSA Assumption: $f_{RSA[N,e]}$ is a OWF collection, when P, Q random k-bit primes and $e < N$ random number s.t. $\gcd(e,\varphi(N))=1$ (with inputs uniformly from $\mathbb{Z}_N$ or $\mathbb{Z}_N^*$)
  - Alternate version: $e=3$, P, Q restricted so that $\gcd(3,\varphi(N))=1$
- RSA Assumption will be false if one can factorize N
  - Then knows $\varphi(N)$ and can find $d=e^{-1}$ in $\mathbb{Z}_{\varphi(N)}^*$
  - Converse not known to hold
- Trapdoor OWP Candidate

Rabin Function

Rabin Function

- $f_{Rabin[N]}(x) = x^2 \bmod N$ where N=PQ, P,Q primes $\equiv 3 \bmod 4$

Rabin Function

- $f_{Rabin[N]}(x) = x^2 \bmod N$ where N=PQ, P,Q primes $\equiv 3 \bmod 4$
  - Candidate OWF collection (indexed by N)

Rabin Function

- $f_{Rabin[N]}(x) = x^2 \bmod N$ where N=PQ, P,Q primes $\equiv 3 \bmod 4$
  - Candidate OWF collection (indexed by N)
    - Equivalent to the assumption that f_{mult} is a OWF (for the appropriate distribution)

Rabin Function

- $f_{Rabin[N]}(x) = x^2 \bmod N$ where N=PQ, P,Q primes $\equiv 3 \bmod 4$
  - Candidate OWF collection (indexed by N)
    - Equivalent to the assumption that f_{mult} is a OWF (for the appropriate distribution)
      - If can factor N, will see how to find square-roots

Rabin Function

- $f_{Rabin[N]}(x) = x^2 \bmod N$ where N=PQ, P,Q primes $\equiv 3 \bmod 4$
  - Candidate OWF collection (indexed by N)
    - Equivalent to the assumption that f_{mult} is a OWF (for the appropriate distribution)
      - If can factor N, will see how to find square-roots
        - So (P,Q) a trapdoor to "invert"

Rabin Function

- $f_{Rabin[N]}(x) = x^2 \bmod N$ where N=PQ, P,Q primes $\equiv 3 \bmod 4$
  - Candidate OWF collection (indexed by N)
    - Equivalent to the assumption that f_{mult} is a OWF (for the appropriate distribution)
      - If can factor N, will see how to find square-roots
        - So (P,Q) a trapdoor to "invert"
      - If can take square-root mod N, can factor N [Exercise]

Rabin Function

- $f_{Rabin[N]}(x) = x^2 \bmod N$ where N=PQ, P,Q primes $\equiv 3 \bmod 4$
  - Candidate OWF collection (indexed by N)
    - Equivalent to the assumption that f_{mult} is a OWF (for the appropriate distribution)
      - If can factor N, will see how to find square-roots
        - So (P,Q) a trapdoor to "invert"
      - If can take square-root mod N, can factor N [Exercise]
  - Not a permutation in $\mathbb{Z}_N$ or $\mathbb{Z}_N^*$ [Why?]

Rabin Function

- $f_{Rabin[N]}(x) = x^2 \bmod N$ where N=PQ, P,Q primes $\equiv 3 \bmod 4$
  - Candidate OWF collection (indexed by N)
    - Equivalent to the assumption that f_{mult} is a OWF (for the appropriate distribution)
      - If can factor N, will see how to find square-roots
        - So (P,Q) a trapdoor to "invert"
      - If can take square-root mod N, can factor N [Exercise]
  - Not a permutation in $\mathbb{Z}_N$ or $\mathbb{Z}_N^*$ [Why?]
    - How about in $\mathbb{QR}_N^*$?

Square-roots in $\mathbb{Z}_p^*$

Square-roots in $\mathbb{Z}_p^*$

- x^2 easy to invert in $\mathbb{Z}_p^*$ if (P-1)/2 odd

Square-roots in $\mathbb{Z}_p^*$

- x^2 easy to invert in $\mathbb{Z}_p^*$ if (P-1)/2 odd
  - Let $y := (x^2)^{(P+1)/4}$ to get $y^2 = x^2$

Square-roots in $\mathbb{Z}_p^*$

- x^2 easy to invert in $\mathbb{Z}_p^*$ if (P-1)/2 odd
  - Let $y := (x^2)^{(P+1)/4}$ to get $y^2 = x^2$
- What are the square-roots?

Square-roots in $\mathbb{Z}_p^*$

- x^2 easy to invert in $\mathbb{Z}_p^*$ if (P-1)/2 odd
  - Let $y := (x^2)^{(P+1)/4}$ to get $y^2 = x^2$
- What are the square-roots?
  - $\sqrt{1} = \pm 1$

Square-roots in $\mathbb{Z}_p^*$

- x^2 easy to invert in $\mathbb{Z}_p^*$ if $(P-1)/2$ odd
  - Let $y := (x^2)^{(P+1)/4}$ to get $y^2 = x^2$
- What are the square-roots?
  - $\sqrt{1} = \pm 1$
  - $x^2=1 \pmod P \Leftrightarrow (x+1)(x-1) = 0 \pmod P \Leftrightarrow (x+1)=0$ or $(x-1)=0 \pmod P$

    $\Leftrightarrow x=1 \pmod P$ or $x=-1 \pmod P$

Square-roots in $\mathbb{Z}_p^*$

- x^2 easy to invert in $\mathbb{Z}_p^*$ if $(P-1)/2$ odd
  - Let $y := (x^2)^{(P+1)/4}$ to get $y^2 = x^2$
- What are the square-roots?
  - $\sqrt{1} = \pm 1$
  - $x^2=1 \pmod P \Leftrightarrow (x+1)(x-1) = 0 \pmod P \Leftrightarrow (x+1)=0$ or $(x-1)=0 \pmod P$

    $\Leftrightarrow x=1 \pmod P$ or $x=-1 \pmod P$
  - $-1 = g^{(P-1)/2}$ because $(g^{(P-1)/2})^2 = 1$ (and $g^{(P-1)/2} \neq 1$, as order(g) = P-1)

Square-roots in $\mathbb{Z}_p^*$

- x^2 easy to invert in $\mathbb{Z}_p^*$ if $(P-1)/2$ odd
  - Let $y := (x^2)^{(P+1)/4}$ to get $y^2 = x^2$
- What are the square-roots?
  - $\sqrt{1} = \pm 1$
  - $x^2=1 \pmod P \Leftrightarrow (x+1)(x-1) = 0 \pmod P \Leftrightarrow (x+1)=0$ or $(x-1)=0 \pmod P$
    $\Leftrightarrow x=1 \pmod P$ or $x=-1 \pmod P$
  - $-1 = g^{(P-1)/2}$ because $(g^{(P-1)/2})^2 = 1$ (and $g^{(P-1)/2} \neq 1$, as order(g) = P-1)
  - More generally $\sqrt{(x^2)} = \pm x$ (i.e., only x and $-1*x$) [Why?]

Square-roots in QR_p^*

Square-roots in QR_p^*

- In $\mathbb{Z}_p^*$ $\sqrt{(x^2)} = \pm x$

Square-roots in $\mathbb{QR}_p^*$

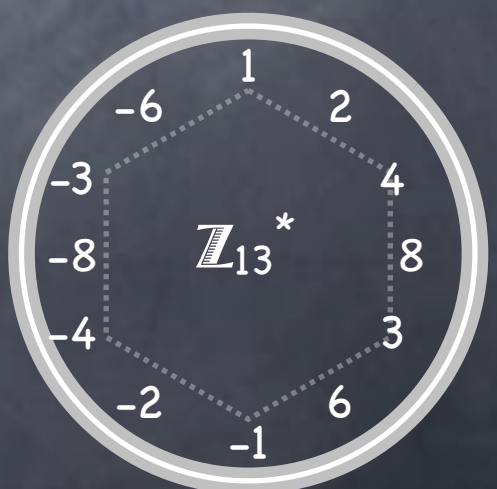
- In $\mathbb{Z}_p^*$ $\sqrt{(x^2)} = \pm x$
- How many square-roots stay in $\mathbb{QR}_p^*$?

Square-roots in $\mathbb{QR}_p^*$

- In $\mathbb{Z}_p^*$ $\sqrt{(x^2)} = \pm x$
- How many square-roots stay in $\mathbb{QR}_p^*$?
  - Depends on P!

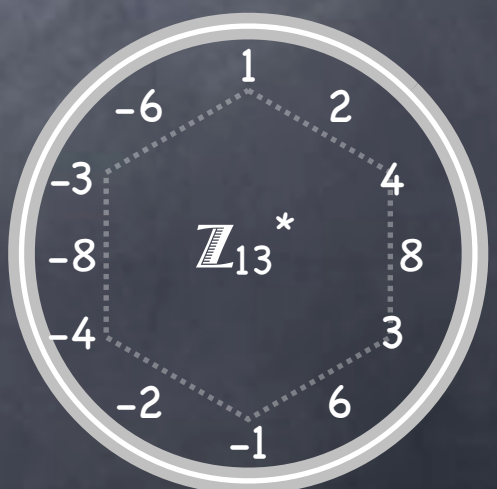
Square-roots in $\mathbb{QR}_p^*$

- In $\mathbb{Z}_p^*$ $\sqrt{(x^2)} = \pm x$
- How many square-roots stay in $\mathbb{QR}_p^*$?
  - Depends on P!
  - e.g. $\mathbb{QR}_{13}^* = \{\pm 1, \pm 3, \pm 4\}$



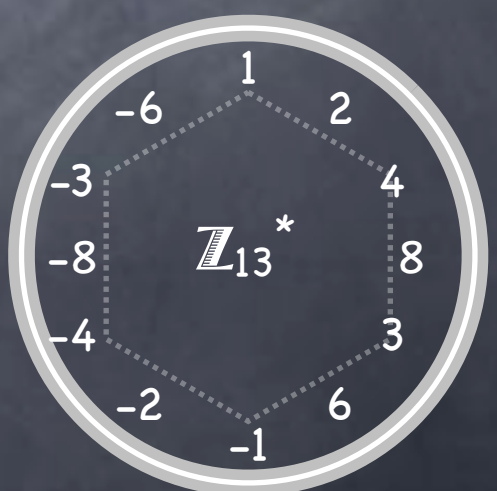
Square-roots in $\mathbb{QR}_p^*$

- In $\mathbb{Z}_p^*$ $\sqrt{(x^2)} = \pm x$
- How many square-roots stay in $\mathbb{QR}_p^*$?
  - Depends on P!
  - e.g. $\mathbb{QR}_{13}^* = \{\pm 1, \pm 3, \pm 4\}$
    - 1,3,-4 have 2 square-roots each. But -1,-3,4 have none within $\mathbb{QR}_{13}^*$



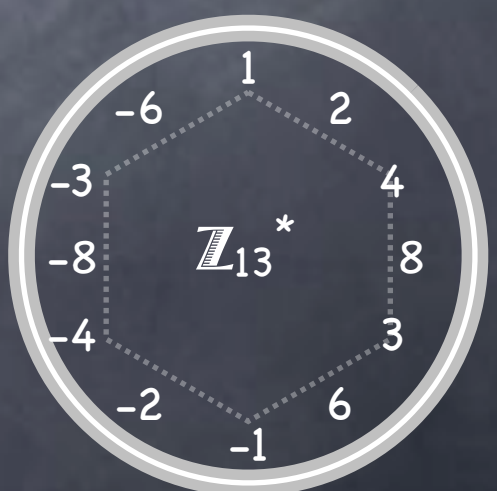
Square-roots in $\mathbb{QR}_p^*$

- In $\mathbb{Z}_p^*$ $\sqrt{(x^2)} = \pm x$
- How many square-roots stay in $\mathbb{QR}_p^*$?
  - Depends on P!
  - e.g. $\mathbb{QR}_{13}^* = \{\pm 1, \pm 3, \pm 4\}$
    - 1,3,-4 have 2 square-roots each. But -1,-3,4 have none within $\mathbb{QR}_{13}^*$
    - Since $-1 \in \mathbb{QR}_{13}^*$, $x \in \mathbb{QR}_{13}^* \Rightarrow -x \in \mathbb{QR}_{13}^*$



Square-roots in $\mathbb{QR}_p^*$

- In $\mathbb{Z}_p^*$ $\sqrt{(x^2)} = \pm x$
- How many square-roots stay in $\mathbb{QR}_p^*$?
  - Depends on P!
  - e.g. $\mathbb{QR}_{13}^* = \{\pm 1, \pm 3, \pm 4\}$
    - 1,3,-4 have 2 square-roots each. But -1,-3,4 have none within $\mathbb{QR}_{13}^*$
    - Since $-1 \in \mathbb{QR}_{13}^*$, $x \in \mathbb{QR}_{13}^* \Rightarrow -x \in \mathbb{QR}_{13}^*$
    - $-1 \in \mathbb{QR}_p^*$ iff (P-1)/2 even

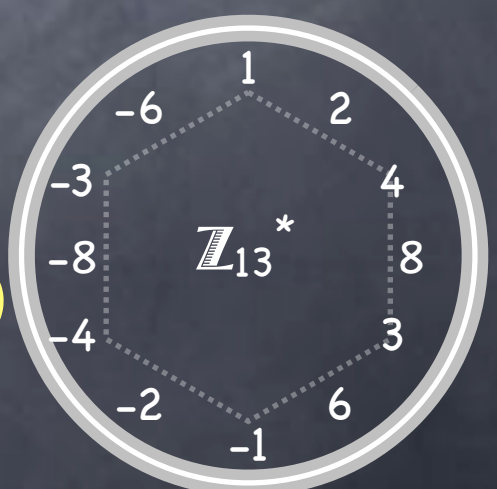


Square-roots in $\mathbb{QR}_p^*$

- In $\mathbb{Z}_p^*$ $\sqrt{(x^2)} = \pm x$
- How many square-roots stay in $\mathbb{QR}_p^*$?
  - Depends on P!
  - e.g. $\mathbb{QR}_{13}^* = \{\pm 1, \pm 3, \pm 4\}$
    - 1,3,-4 have 2 square-roots each. But -1,-3,4 have none within $\mathbb{QR}_{13}^*$
    - Since $-1 \in \mathbb{QR}_{13}^*$, $x \in \mathbb{QR}_{13}^* \Rightarrow -x \in \mathbb{QR}_{13}^*$
    - $-1 \in \mathbb{QR}_p^*$ iff (P-1)/2 even
- If (P-1)/2 odd, exactly one of $\pm x$ in $\mathbb{QR}_p^*$ (for all x)

Square-roots in $\mathbb{QR}_p^*$

- In $\mathbb{Z}_p^*$ $\sqrt{(x^2)} = \pm x$
- How many square-roots stay in $\mathbb{QR}_p^*$?
  - Depends on P!
  - e.g. $\mathbb{QR}_{13}^* = \{\pm 1, \pm 3, \pm 4\}$
    - 1,3,-4 have 2 square-roots each. But -1,-3,4 have none within $\mathbb{QR}_{13}^*$
    - Since $-1 \in \mathbb{QR}_{13}^*$, $x \in \mathbb{QR}_{13}^* \Rightarrow -x \in \mathbb{QR}_{13}^*$
    - $-1 \in \mathbb{QR}_p^*$ iff (P-1)/2 even
- If (P-1)/2 odd, exactly one of $\pm x$ in $\mathbb{QR}_p^*$ (for all x)
  - Then, squaring is a permutation in $\mathbb{QR}_p^*$



Square-roots in QR_p^*

Square-roots in QR_p^*

- In $\mathbb{Z}_p^*$ $\sqrt{(x^2)} = \pm x$ (i.e., x and $-1*x$)

Square-roots in $\mathbb{QR}_p^*$

- In $\mathbb{Z}_p^*$ $\sqrt{(x^2)} = \pm x$ (i.e., x and $-1*x$)
- If (P-1)/2 odd, squaring is a permutation in $\mathbb{QR}_p^*$

Square-roots in QR_p^*

- In $\mathbb{Z}_p^*$ $\sqrt{(x^2)} = \pm x$ (i.e., x and $-1*x$)
- If (P-1)/2 odd, squaring is a permutation in QR_p^*
- But easy to compute both ways

Square-roots in $\mathbb{QR}_p^*$

- In $\mathbb{Z}_p^*$ $\sqrt{(x^2)} = \pm x$ (i.e., x and $-1*x$)
- If $(P-1)/2$ odd, squaring is a permutation in $\mathbb{QR}_p^*$
- But easy to compute both ways
  - In fact $\sqrt{z} = z^{(P+1)/4} \in \mathbb{QR}_p^*$ (because $(P+1)/2$ even)

Square-roots in $\mathbb{QR}_p^*$

- In $\mathbb{Z}_p^*$ $\sqrt{(x^2)} = \pm x$ (i.e., x and $-1*x$)
- If (P-1)/2 odd, squaring is a permutation in $\mathbb{QR}_p^*$
- But easy to compute both ways
  - In fact $\sqrt{z} = z^{(P+1)/4} \in \mathbb{QR}_p^*$ (because (P+1)/2 even)
- Rabin function defined in $\mathbb{QR}_N^*$ and relies on keeping the factorization of N=PQ hidden


QR_N*

QR_N^*

- What do elements in QR_N^* look like, for N=PQ?

QR_N^*

- What do elements in QR_N^* look like, for N=PQ?
  - By CRT, can write $a \in \mathbb{Z}_N^*$ as $(x,y) \in \mathbb{Z}_P^* \times \mathbb{Z}_Q^*$

$\mathbb{QR}_N^*$

- What do elements in $\mathbb{QR}_N^*$ look like, for N=PQ?
  - By CRT, can write $a \in \mathbb{Z}_N^*$ as $(x,y) \in \mathbb{Z}_P^* \times \mathbb{Z}_Q^*$
  - CRT representation of a^2 is $(x^2,y^2) \in \mathbb{QR}_P^* \times \mathbb{QR}_Q^*$

QR_N^*

- What do elements in QR_N^* look like, for N=PQ?
  - By CRT, can write $a \in Z_N^*$ as $(x,y) \in Z_P^* \times Z_Q^*$
  - CRT representation of a^2 is $(x^2,y^2) \in QR_P^* \times QR_Q^*$
  - $QR_N^* \cong QR_P^* \times QR_Q^*$

QR_N^*

- What do elements in QR_N^* look like, for N=PQ?
  - By CRT, can write $a \in Z_N^*$ as $(x,y) \in Z_P^* \times Z_Q^*$
  - CRT representation of a^2 is $(x^2,y^2) \in QR_P^* \times QR_Q^*$
  - $QR_N^* \cong QR_P^* \times QR_Q^*$
  - If both $P,Q \equiv 3 \pmod 4$, then squaring is a permutation in QR_N^*

$\mathbb{QR}_N^*$

- What do elements in $\mathbb{QR}_N^*$ look like, for N=PQ?
  - By CRT, can write $a \in \mathbb{Z}_N^*$ as $(x,y) \in \mathbb{Z}_P^* \times \mathbb{Z}_Q^*$
  - CRT representation of a^2 is $(x^2,y^2) \in \mathbb{QR}_P^* \times \mathbb{QR}_Q^*$
  - $\mathbb{QR}_N^* \cong \mathbb{QR}_P^* \times \mathbb{QR}_Q^*$
  - If both $P,Q \equiv 3 \pmod 4$, then squaring is a permutation in $\mathbb{QR}_N^*$
    - $\sqrt{(x^2,y^2)} = (\pm x, \pm y)$ in $\mathbb{Z}_P^* \times \mathbb{Z}_Q^*$ but exactly one in $\mathbb{QR}_P^* \times \mathbb{QR}_Q^*$

$\mathbb{QR}_N^*$

- What do elements in $\mathbb{QR}_N^*$ look like, for N=PQ?
  - By CRT, can write $a \in \mathbb{Z}_N^*$ as $(x,y) \in \mathbb{Z}_P^* \times \mathbb{Z}_Q^*$
  - CRT representation of a^2 is $(x^2,y^2) \in \mathbb{QR}_P^* \times \mathbb{QR}_Q^*$
  - $\mathbb{QR}_N^* \cong \mathbb{QR}_P^* \times \mathbb{QR}_Q^*$
  - If both $P,Q \equiv 3 \pmod 4$, then squaring is a permutation in $\mathbb{QR}_N^*$
    - $\sqrt{(x^2,y^2)} = (\pm x, \pm y)$ in $\mathbb{Z}_P^* \times \mathbb{Z}_Q^*$ but exactly one in $\mathbb{QR}_P^* \times \mathbb{QR}_Q^*$
    - Can efficiently do this, if can compute (and invert) the isomorphism from $\mathbb{QR}_N^*$ to $\mathbb{QR}_P^* \times \mathbb{QR}_Q^*$

$\mathbb{QR}_N^*$

- What do elements in $\mathbb{QR}_N^*$ look like, for N=PQ?
  - By CRT, can write $a \in \mathbb{Z}_N^*$ as $(x,y) \in \mathbb{Z}_P^* \times \mathbb{Z}_Q^*$
  - CRT representation of a^2 is $(x^2,y^2) \in \mathbb{QR}_P^* \times \mathbb{QR}_Q^*$
  - $\mathbb{QR}_N^* \cong \mathbb{QR}_P^* \times \mathbb{QR}_Q^*$
  - If both $P,Q \equiv 3 \pmod 4$, then squaring is a permutation in $\mathbb{QR}_N^*$
    - $\sqrt{(x^2,y^2)} = (\pm x, \pm y)$ in $\mathbb{Z}_P^* \times \mathbb{Z}_Q^*$ but exactly one in $\mathbb{QR}_P^* \times \mathbb{QR}_Q^*$
    - Can efficiently do this, if can compute (and invert) the isomorphism from $\mathbb{QR}_N^*$ to $\mathbb{QR}_P^* \times \mathbb{QR}_Q^*$
      - (P,Q) is a trapdoor

$\mathbb{QR}_N^*$

- What do elements in $\mathbb{QR}_N^*$ look like, for N=PQ?
  - By CRT, can write $a \in \mathbb{Z}_N^*$ as $(x,y) \in \mathbb{Z}_P^* \times \mathbb{Z}_Q^*$
  - CRT representation of a^2 is $(x^2,y^2) \in \mathbb{QR}_P^* \times \mathbb{QR}_Q^*$
  - $\mathbb{QR}_N^* \cong \mathbb{QR}_P^* \times \mathbb{QR}_Q^*$
  - If both $P,Q \equiv 3 \pmod 4$, then squaring is a permutation in $\mathbb{QR}_N^*$
    - $\sqrt{(x^2,y^2)} = (\pm x, \pm y)$ in $\mathbb{Z}_P^* \times \mathbb{Z}_Q^*$ but exactly one in $\mathbb{QR}_P^* \times \mathbb{QR}_Q^*$
    - Can efficiently do this, if can compute (and invert) the isomorphism from $\mathbb{QR}_N^*$ to $\mathbb{QR}_P^* \times \mathbb{QR}_Q^*$
      - (P,Q) is a trapdoor
    - Without trapdoor, OWF candidate ($\mathbb{QR}_N^*$ forms $1/4^{th}$ of $\mathbb{Z}_N^*$)

Rabin Function

Rabin Function

- $f_{Rabin[N]}(x) = x^2 \bmod N$

Rabin Function

- $f_{Rabin[N]}(x) = x^2 \bmod N$
  - Candidate OWF collection, with N=PQ (P,Q random k-bit primes)

Rabin Function

- $f_{Rabin[N]}(x) = x^2 \bmod N$
  - Candidate OWF collection, with N=PQ (P,Q random k-bit primes)
  - If P, Q ≡3 (mod 4), then in $\mathbb{QR}_N^*$

Rabin Function

- $f_{Rabin[N]}(x) = x^2 \bmod N$
  - Candidate OWF collection, with N=PQ (P,Q random k-bit primes)
  - If P, Q ≡3 (mod 4), then in $\mathbb{QR}_N^*$
    - A permutation

Rabin Function

- $f_{Rabin[N]}(x) = x^2 \bmod N$
  - Candidate OWF collection, with N=PQ (P,Q random k-bit primes)
  - If P, Q $\equiv 3 \pmod 4$, then in $\mathbb{QR}_N^*$
    - A permutation
    - Has a trapdoor for inverting (namely (P,Q))

Rabin Function

- $f_{Rabin[N]}(x) = x^2 \bmod N$
  - Candidate OWF collection, with N=PQ (P,Q random k-bit primes)
  - If P, Q $\equiv 3 \pmod 4$, then in $\mathbb{QR}_N^*$
    - A permutation
    - Has a trapdoor for inverting (namely (P,Q))
- Candidate Trapdoor OWP

Summary

Summary

- A DLA candidate: $\mathbb{Z}_p^*$

Summary

- A DLA candidate: $\mathbb{Z}_p^*$
- A DDH candidate: $\mathbb{QR}_p^*$ where P is a safe prime

Summary

- A DLA candidate: $\mathbb{Z}_p^*$
- A DDH candidate: $\mathbb{QR}_p^*$ where P is a safe prime
- Chinese Remainder Theorem

Summary

- A DLA candidate: $\mathbb{Z}_P^*$
- A DDH candidate: $\mathbb{QR}_P^*$ where P is a safe prime
- Chinese Remainder Theorem
  - $\mathbb{Z}_N \cong \mathbb{Z}_P \times \mathbb{Z}_Q$

Summary

- A DLA candidate: $\mathbb{Z}_p^*$
- A DDH candidate: $\mathbb{QR}_p^*$ where P is a safe prime
- Chinese Remainder Theorem
  - $\mathbb{Z}_N \cong \mathbb{Z}_p \times \mathbb{Z}_q$
  - $\mathbb{Z}_N^* \cong \mathbb{Z}_p^* \times \mathbb{Z}_q^*$

Summary

- A DLA candidate: $\mathbb{Z}_P^*$
- A DDH candidate: $\mathbb{QR}_P^*$ where P is a safe prime
- Chinese Remainder Theorem
  - $\mathbb{Z}_N \cong \mathbb{Z}_P \times \mathbb{Z}_Q$
  - $\mathbb{Z}_N^* \cong \mathbb{Z}_P^* \times \mathbb{Z}_Q^*$
  - $\mathbb{QR}_N^* \cong \mathbb{QR}_P^* \times \mathbb{QR}_Q^*$

Summary

- A DLA candidate: $\mathbb{Z}_P^*$
- A DDH candidate: $\mathbb{QR}_P^*$ where P is a safe prime
- Chinese Remainder Theorem
  - $\mathbb{Z}_N \cong \mathbb{Z}_P \times \mathbb{Z}_Q$
  - $\mathbb{Z}_N^* \cong \mathbb{Z}_P^* \times \mathbb{Z}_Q^*$
  - $\mathbb{QR}_N^* \cong \mathbb{QR}_P^* \times \mathbb{QR}_Q^*$
- T-OWP candidates:

Summary

- A DLA candidate: $\mathbb{Z}_P^*$
- A DDH candidate: $\mathbb{QR}_P^*$ where P is a safe prime
- Chinese Remainder Theorem
  - $\mathbb{Z}_N \cong \mathbb{Z}_P \times \mathbb{Z}_Q$
  - $\mathbb{Z}_N^* \cong \mathbb{Z}_P^* \times \mathbb{Z}_Q^*$
  - $\mathbb{QR}_N^* \cong \mathbb{QR}_P^* \times \mathbb{QR}_Q^*$
- T-OWP candidates:
  - $f_{RSA[N,e]} = x^e \bmod N$ where $N=PQ$ and $\gcd(e,\varphi(N))=1$

Summary

- A DLA candidate: $\mathbb{Z}_P^*$
- A DDH candidate: $\mathbb{QR}_P^*$ where P is a safe prime
- Chinese Remainder Theorem
  - $\mathbb{Z}_N \cong \mathbb{Z}_P \times \mathbb{Z}_Q$
  - $\mathbb{Z}_N^* \cong \mathbb{Z}_P^* \times \mathbb{Z}_Q^*$
  - $\mathbb{QR}_N^* \cong \mathbb{QR}_P^* \times \mathbb{QR}_Q^*$
- T-OWP candidates:
  - $f_{RSA[N,e]} = x^e \bmod N$ where $N=PQ$ and $\gcd(e,\varphi(N))=1$
    - Trapdoor: $(P,Q) \rightarrow \varphi(N) \rightarrow d=e^{-1}$ in $\mathbb{Z}_{\varphi(N)}^*$

Summary

- A DLA candidate: $\mathbb{Z}_P^*$
- A DDH candidate: $\mathbb{QR}_P^*$ where P is a safe prime
- Chinese Remainder Theorem
  - $\mathbb{Z}_N \cong \mathbb{Z}_P \times \mathbb{Z}_Q$
  - $\mathbb{Z}_N^* \cong \mathbb{Z}_P^* \times \mathbb{Z}_Q^*$
  - $\mathbb{QR}_N^* \cong \mathbb{QR}_P^* \times \mathbb{QR}_Q^*$
- T-OWP candidates:
  - $f_{RSA[N,e]} = x^e \bmod N$ where $N=PQ$ and $\gcd(e,\varphi(N))=1$
    - Trapdoor: $(P,Q) \rightarrow \varphi(N) \rightarrow d=e^{-1}$ in $\mathbb{Z}_{\varphi(N)}^*$
  - $f_{Rabin[N]} = x^2 \bmod N$ where $N=PQ$, where $P,Q \equiv 3 \pmod 4$

Summary

- A DLA candidate: $\mathbb{Z}_P^*$
- A DDH candidate: $\mathbb{QR}_P^*$ where P is a safe prime
- Chinese Remainder Theorem
  - $\mathbb{Z}_N \cong \mathbb{Z}_P \times \mathbb{Z}_Q$
  - $\mathbb{Z}_N^* \cong \mathbb{Z}_P^* \times \mathbb{Z}_Q^*$
  - $\mathbb{QR}_N^* \cong \mathbb{QR}_P^* \times \mathbb{QR}_Q^*$
- T-OWP candidates:
  - $f_{RSA[N,e]} = x^e \bmod N$ where N=PQ and gcd(e,φ(N))=1
    - Trapdoor: (P,Q) → φ(N) → $d=e^{-1}$ in $\mathbb{Z}_{\varphi(N)}^*$
  - $f_{Rabin[N]} = x^2 \bmod N$ where N=PQ, where P,Q ≡3 (mod 4)
    - Trapdoor: (P,Q)