Public-Key Cryptography

Lecture 10

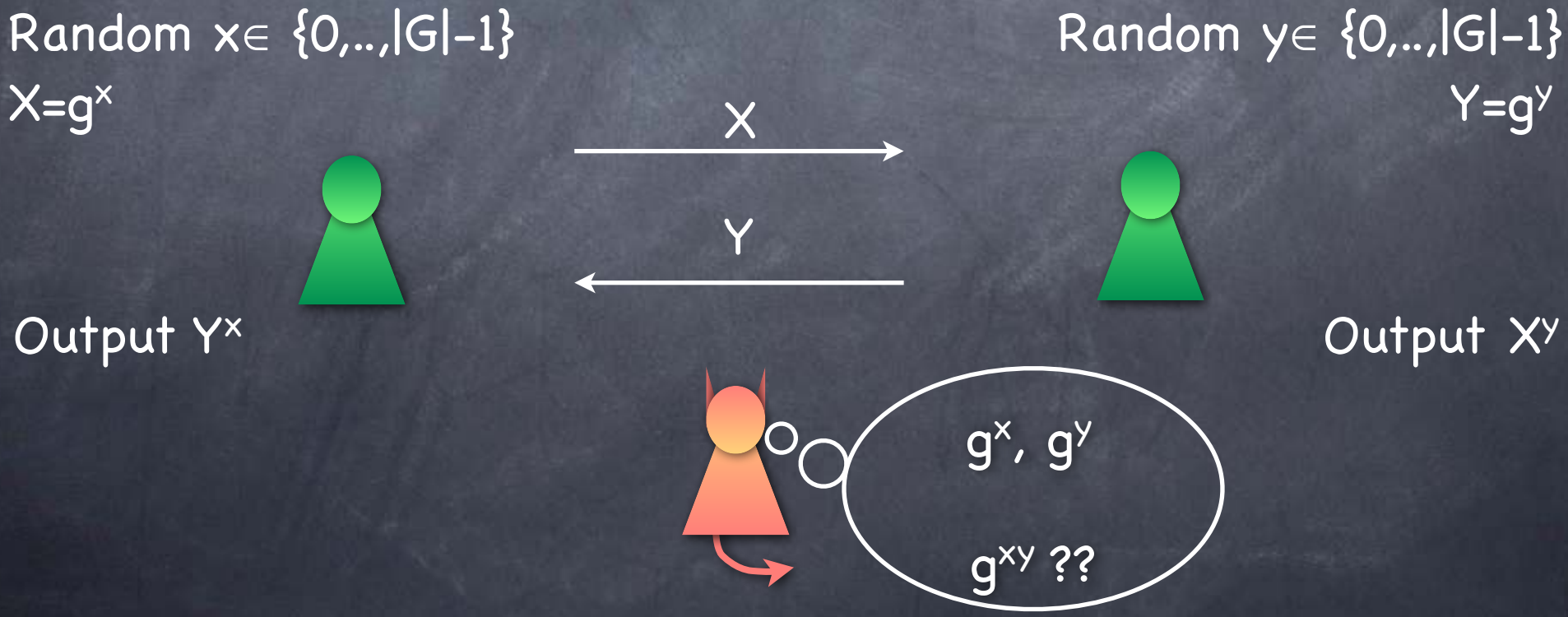
DDH Assumption

El Gamal Encryption

Public-Key Encryption from Trapdoor OWP

Diffie-Hellman Key-exchange

- "Secure" under DDH: $(g^x, g^x, g^{xy}) \approx (g^x, g^x, g^r)$



Decisional Diffie-Hellman (DDH) Assumption

- $\{(g^x, g^y, g^{xy})\}_{(G,g)\leftarrow\textbf{GroupGen}; x,y\leftarrow[|G|]} \approx \{(g^x, g^y, g^r)\}_{(G,g)\leftarrow\textbf{GroupGen}; x,y,r\leftarrow[|G|]}$
- At least as strong as Discrete Log Assumption (DLA)
  - DLA: Raise(x; G,g) = (g^x; G,g) is a OWF collection
  - If DDH assumption holds, then DLA holds [Why?]
- 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!
- Do we have a candidate group for DDH?

A Candidate DDH Group

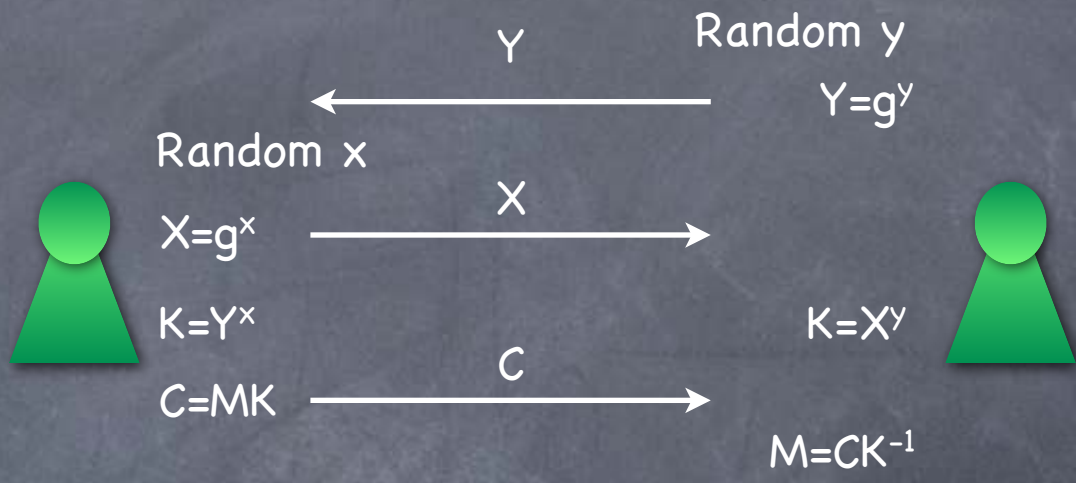
- Consider $\mathbb{QR}_P^*$: subgroup of Quadratic Residues ("even power" elements) of $\mathbb{Z}_P^*$

- Easy to check if an element is a QR or not: check if raising to |G|/2 gives 1 (identity element)
- DDH does not hold in $\mathbb{Z}_P^*$: g^{xy} is a QR w/ prob. 3/4; g^z is QR only w/ prob. 1/2.
- How about in $\mathbb{QR}_P^*$?
  - Could check if cubic residue in $\mathbb{Z}_P^*$!
    - But if (P-1) is not divisible by 3, all elements in $\mathbb{Z}_P^*$ are cubic residues!
  - "Safe" if (P-1)/2 is also prime: P called a safe-prime

DDH Candidate:
$\mathbb{QR}_P^*$
where P is a safe-prime

El Gamal Encryption

- Based on DH key-exchange
  - Alice, Bob generate a key using DH key-exchange
  - Then use it as a one-time pad
- Bob's "message" in the key-exchange is his PK
- Alice's message in the key-exchange and the ciphertext of the one-time pad together form a single ciphertext



KeyGen: $PK=(G,g,Y)$, $SK=(G,g,y)$

$Enc_{(G,g,Y)}(M) = (X=g^x, C=MY^x)$

$Dec_{(G,g,y)}(X,C) = CX^{-y}$

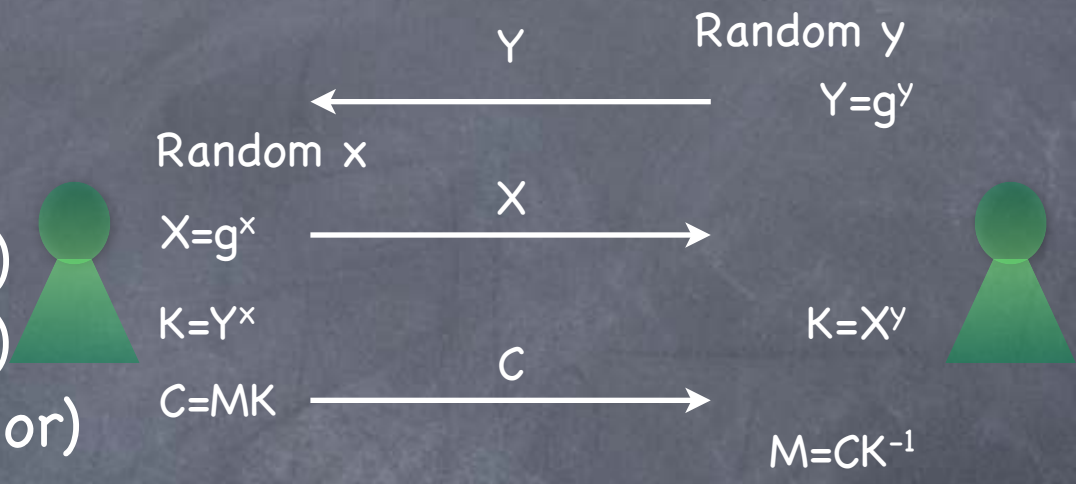
- KeyGen uses GroupGen to get (G,g)
- x, y uniform from $\mathbb{Z}_{|G|}$
- Message encoded into group element, and decoded

Security of El Gamal

- El Gamal IND-CPA secure if DDH holds (for the collection of groups used)
  - Construct a DDH adversary A* given an IND-CPA adversary A
  - A*(G,g; g^x,g^y,g^z) (where (G,g) ← GroupGen, x,y random and z=xy or random) plays the IND-CPA experiment with A:
    - But sets PK=(G,g,g^y) and Enc(M_b)=(g^x,$M_b g^z$)
    - Outputs 1 if experiment outputs 1 (i.e. if b=b')
  - When z=random, A* outputs 1 with probability = 1/2
  - When z=xy, exactly IND-CPA experiment: A* outputs 1 with probability = 1/2 + advantage of A.

Abstracting El Gamal

- Trapdoor PRG:
  - KeyGen: a pair (PK,SK)
  - Three functions: $G_{PK}(.)$ (a PRG) and $T_{PK}(.)$ (make trapdoor info) and $R_{SK}(.)$ (opening the trapdoor)
    - $G_{PK}(x)$ is pseudorandom even given $T_{PK}(x)$ and PK
    - $(PK, T_{PK}(x), G_{PK}(x)) \approx (PK, T_{PK}(x), r)$
    - $T_{PK}(x)$ hides $G_{PK}(x)$. SK opens it.
      - $R_{SK}(T_{PK}(x)) = G_{PK}(x)$
- Enough for an IND-CPA secure PKE scheme (e.g., Security of El Gamal)



KeyGen: PK=(G,g,Y), SK=(G,g,y)

$Enc_{(G,g,Y)}(M) = (X=g^x, C=MY^x)$

$Dec_{(G,g,y)}(X,C) = CX^{-y}$

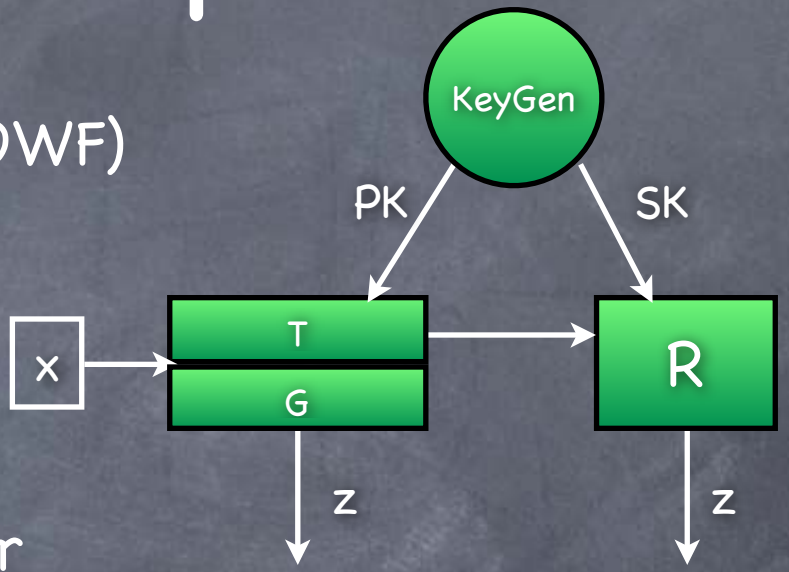
KeyGen: (PK,SK)

$Enc_{PK}(M) = (X=T_{PK}(x), C=M.G_{PK}(x))$

$Dec_{SK}(X,C) = C/R_{SK}(T_{PK}(x))$

Trapdoor PRG from Generic Assumption?

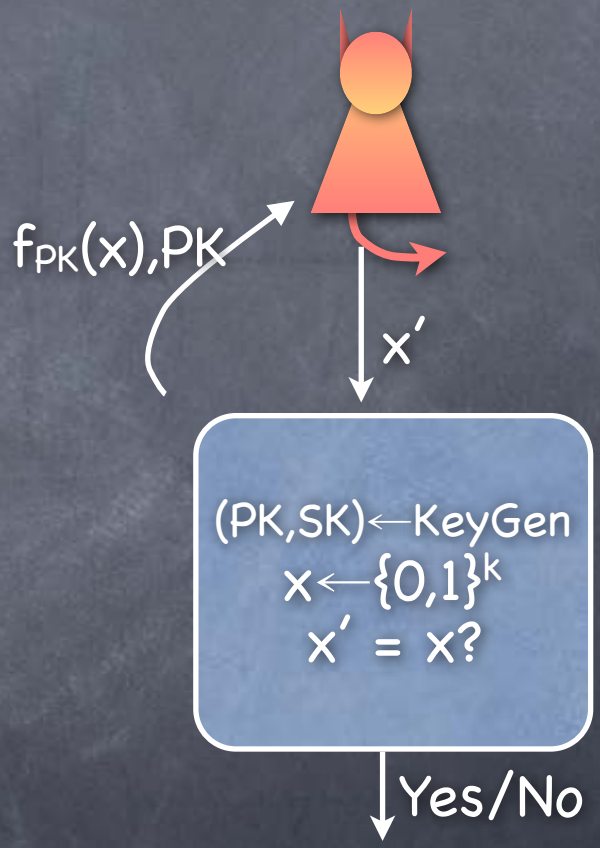
- PRG constructed from OWP (or OWF)
  - Allows us to instantiate the construction with several candidates
- Is there a similar construction for TPRG from OWP?
  - Trapdoor property seems fundamentally different: generic OWP does not suffice
  - Will start with "Trapdoor OWP"



$(PK, T_{PK}(x), G_{PK}(x)) \approx (PK, T_{PK}(x), r)$

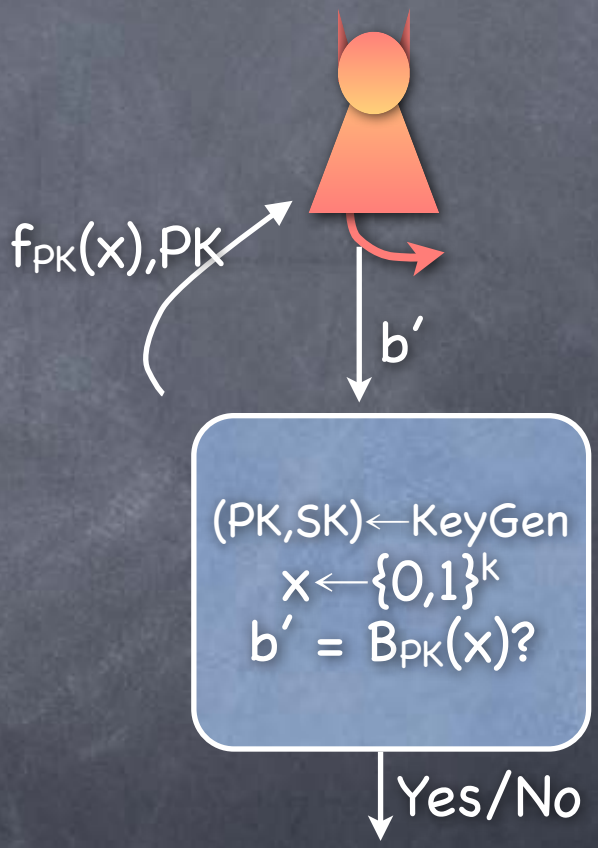
Trapdoor OWP

- (KeyGen,f,f') (all PPT) is a trapdoor one-way permutation if
  - For all (PK,SK) ←KeyGen
    - f_{PK} a permutation
    - f'_{SK} is the inverse of f_{PK}
  - For all PPT adversary, probability of success in the Trapdoor OWP experiment is negligible



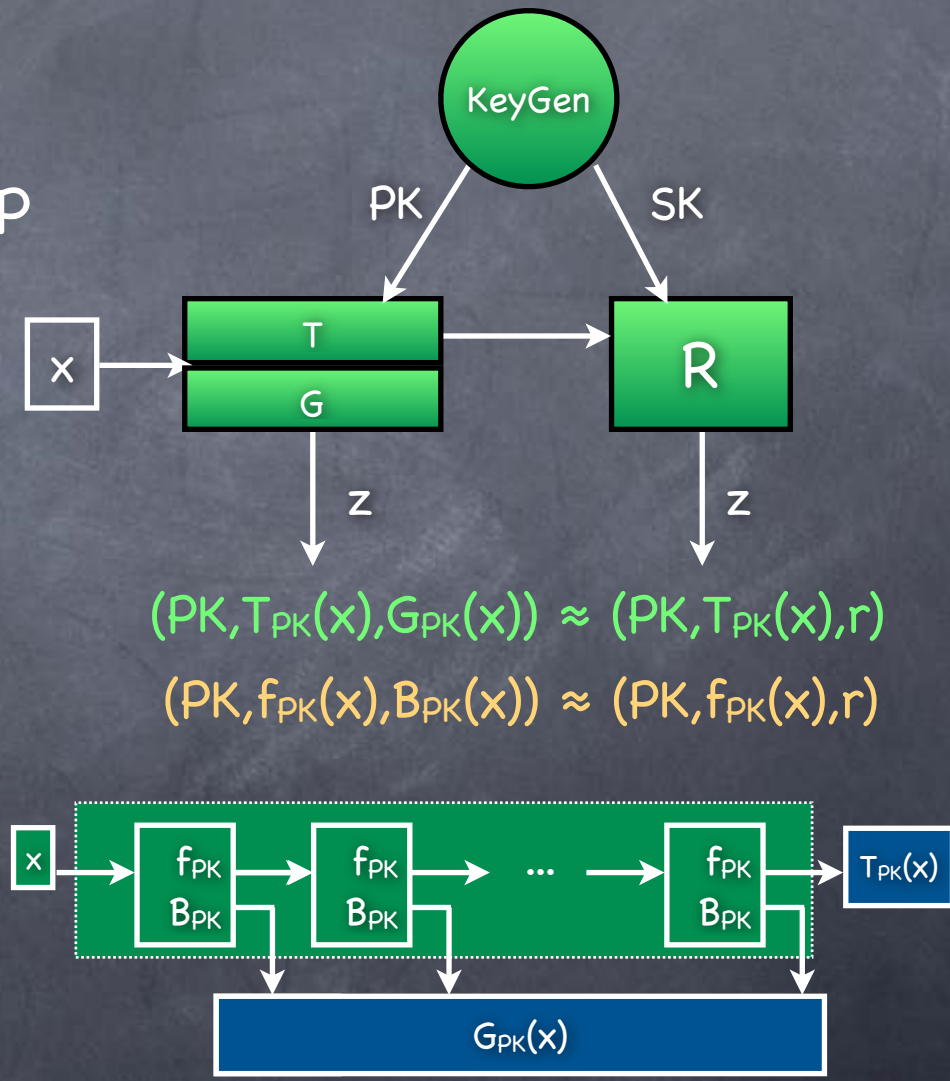
Trapdoor OWP

- (KeyGen,f,f') (all PPT) is a trapdoor one-way permutation if
  - For all (PK,SK) ←KeyGen
    - f_{PK} a permutation
    - f'_{SK} is the inverse of f_{PK}
  - For all PPT adversary, probability of success in the Trapdoor OWP experiment is negligible
  - Hardcore predicate:
    - B_{PK} s.t. $(PK, f_{PK}(x), B_{PK}(x)) \approx (PK, f_{PK}(x), r)$



Trapdoor PRG from Trapdoor OWP

- Same construction as PRG from OWP
- One bit Trapdoor PRG
  - KeyGen same as Trapdoor OWP's KeyGen
  - $G_{PK}(x) := B_{PK}(x)$. $T_{PK}(x) := f_{PK}(x)$. $R_{SK}(y) := G_{PK}(f'_{SK}(y))$
    - (SK assumed to contain PK)
- More generally, last permutation output serves as T_{PK}



Candidate Trapdoor OWPs

- From some (candidate) OWP collections, with index as public-key
- Recall candidate OWF collections
  - Rabin OWF: $f_{Rabin}(x; N) = x^2 \bmod N$, where N = PQ, and P, Q are k-bit primes (and x uniform from {0...N-1})
    - Fact: $f_{Rabin}(.; N)$ is a permutation among quadratic residues, when P, Q are $\equiv 3 \pmod 4$
    - Fact: Can invert $f_{Rabin}(.; N)$ given factorization of N
  - RSA function: $f_{RSA}(x; N,e) = x^e \bmod N$ where N=PQ, P,Q k-bit primes, e s.t. $\gcd(e,\varphi(N)) = 1$ (and x uniform from {0...N-1})

Coming up

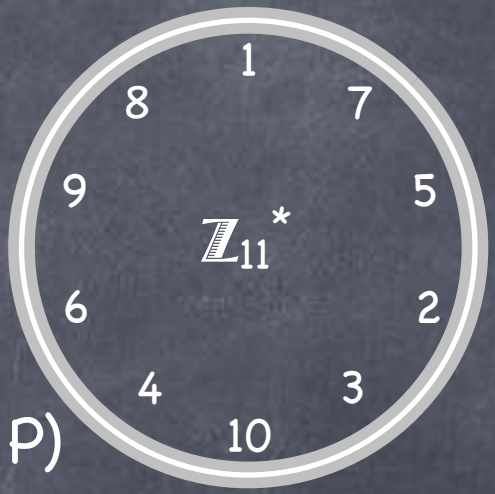
  - Fact: $f_{RSA}(.; N,e)$ is a permutation
  - Fact: While picking (N,e), can also pick d s.t. $x^{ed} = x$

$\mathbb{Z}_N^*$

- 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



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

- e.g. $\mathbb{Z}_{15}^* = \{1,2,4,7,8,11,13,14\}$
  - $\varphi(15) = 8$
- Group operation and inverse efficiently computable
- 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

Also works with P, Q co-primes

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 $\mathbb{Z}_N$

- 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 $\mathbb{Z}_N^*$

- Elements in $\mathbb{Z}_N^*$
  - Multiplication (and identity, and inverse) also coordinate-wise
  - No multiplicative inverse iff (0,b) or (a,0)
  - Else in $\mathbb{Z}_N^*$: i.e., (a,b) s.t. $a \in \mathbb{Z}_P^*$, $b \in \mathbb{Z}_Q^*$
    - $\mathbb{Z}_N^* \cong \mathbb{Z}_P^* \times \mathbb{Z}_Q^*$
  - $\varphi(N) = |\mathbb{Z}_N^*| = (P-1)(Q-1)$ ($P \neq Q$, primes)
- Can efficiently 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

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