Subgroups - theorems

- **Theorem 8.2.5. Cyclic Subgroup Theorem**
  - Let G be a cyclic group. Then every element a ∈ G with ord(a) = s is the primitive element of a cyclic subgroup with s elements.
  - Example
    - $\mathbb{Z}_{11}^{*}$, a = 3, s = ord(3) = 5, H = {1,3,4,5,9}
    - H is a finite, cyclic subgroup of order 5

March 25 Diffie-Hellman Key Exchange 39

39

Subgroups - theorems

- **Theorem 8.2.6. Lagrange's theorem.**
  - Let H be a subgroup of G. Then $|H|$ divides $|G|$.
- Example: $\mathbb{Z}_{11}^{*}$
  - $|\mathbb{Z}_{11}^{*}| = 10$ whose divisors are 1, 2, 5 (and 10)

Subgroup	elements	primitive element
H_1	{1}	$\alpha = 1$
H_2	{1, 10}	$\alpha = 10$
H_5	{1, 3, 4, 5, 9}	$\alpha = 3, 4, 5, 9$

March 25 Diffie-Hellman Key Exchange 40

40

Subgroups - theorems

- **Theorem 8.2.7**
  - Let *G* be a finite cyclic group of order *n* and let α be a generator of *G*. Then for every integer *k* that divides *n* there exists exactly one cyclic subgroup *H* of *G* of order *k*. This subgroup is generated by $\alpha^{n/k}$. *H* consists exactly of the elements $a \in G$ which satisfy the condition $a^k = 1$. There are no other subgroups.
- Example.
  - Given $\mathbb{Z}_{11}^*$, generator $\alpha = 8$ and k = 2, then $\beta = 8^{10/2} = 10 \bmod 11$ is a generator for H of order k = 2

March 25 Diffie-Hellman Key Exchange 41

41

Subgroups vs DLP

- Pohlig-Hellman Algorithm
  - Exploit factorization of $|G| = p_1^{e1} \cdot p_2^{e2} \cdot \ldots \cdot p_\ell^{e\ell}$
  - Run time depends on the size of prime factors
    - The largest prime factor must be in the range 2^{160}
  - Then $|\mathbb{Z}_p^*| = p - 1$ is even ➔ 2 (small) is one of the divisors! ➔ It is advisable to work in a large prime subgroup H
    - If |H| is prime, $\forall a \in H$, a is a generator (Theorem 8.2.4)

March 25 Diffie-Hellman Key Exchange 42

42

Safe primes vs DLP [➔]

- Definition: given a prime p = 2·q+1, where q is a prime then p is a *safe prime* and q is a *Sophie Germain prime.*
  - Examples
    - 5 = 2 x 2 + 1
    - 11 = 2 x 5 + 1
    - 23 = 2 x 11 + 1
- Given It follows that $\mathbb{Z}_p^*$, if p is a safe prime ➔ (p – 1) = 2xq
- It follows that $\mathbb{Z}_p^*$ has a subgroup H_q of (large) prime order q

March 25 Diffie-Hellman Key Exchange 43

43

Safe primes vs DLP [■]

- Given $\mathbb{Z}_p^*$, if p is a safe prime ➔
- (p – 1) = 2 x q, with q prime
- Pohling-Hellman decomposes DLP in $\mathbb{Z}_p^*$ into DLP in H_2 and H_q
  - Solving DLP in H_2 is «easy»
  - Solving DLP in H_q is $O(\sqrt{q})$.
    - As $q = (p-1)/2$ is in the same order as p, then solving DLP in H_q is $\sim O(\sqrt{p})$.

March 25 Diffie-Hellman Key Exchange 44

44

If prime factor is small, DLP is easy in that group you move to.

- The LARGEST factor of $|G|$ must be in the range of 2^{160}.

Smaller factors don't contribute in a meaningful way to complexity.

Idea is choose $p = 2q+1$. So $p-1$ is $2q$, so q determines complexity.

We also know that if I have $\mathbb{Z}_p^*$ such that $|\mathbb{Z}_p^*|$, you have a subset whose cardinality divides $|\mathbb{Z}_p^*|$.

$\mathbb{Z}_p^*$ with p safe prime, gives two subgroups H_2 and H_q. H_q is safe because p is prime and $|H_q|$ is q.

This avoids the small subgroup confinement attack.

Small Subgroup Confinement Attack

- A (small) subgroup confinement attack on a cryptographic method that operates in a large finite group is where an attacker attempts to compromise the method by forcing a key to be confined to an unexpectedly small subgroup of the desired group.
- The Small Subgroup Confinement Attack exploits Theorem 8.2.7

March 25 Diffie-Hellman Key Exchange 45

45

Small Subgroup Confinement Attack against DHKE

- Consider prime p, $\mathbb{Z}_p^*$, and generator α

Alice	MIM	Bob
a ← random()		b ← random()
$A \equiv \alpha^a \bmod p$		$B \equiv \alpha^b \bmod p$
	------A-------------A'-------- >	
		K = $(A')^b$ mod p
	<-------B'---------------------B-----	
K = $(B')^a$ mod p		
	< ------------------ E_K(*session*)--------------------- >	

March 25 Diffie-Hellman Key Exchange 46

46

- Alice and Bob generate private key.
- Both compute public key.
- Alice transmits A, but MIM modifies it into A', same for B into B'.

Small Subgroup Confinement Attack against DHKE

- Recall THEOREM 8.2.7
- The attack
  - Consider k that divides n = $|\mathbb{Z}_p^*|$ = p – 1 ➔
  - A' ≡ $A^{n/k} \equiv (\alpha^a)^{n/k} \equiv (\alpha^{n/k})^a$ mod p
  - B' ≡ $B^{n/k} \equiv (\alpha^b)^{n/k} \equiv (\alpha^{n/k})^b$ mod p
  - Session key K = β^{ab} mod p, with $\beta = \alpha^{n/k}$
  - $\beta = \alpha^{n/k}$ is a generator of subgroup H_k of order k ➔ DHKE gets confined in H_k and brute force becomes easier
  - It is advisable to work in a large prime subgroup H_k

March 25 Diffie-Hellman Key Exchange 47

47

Subgroups vs Key Entropy

- In the DHKEP, the key is defined as $K = H(g^{a \cdot b})$ where *H*(•) is a cryptographic hash function.
  - A practical choice is SHA-256
- Motivation: g^{ab} may not have enough entropy
  - If DHKEP is run in a subgroup Γ of $\mathbb{Z}_p^*$, then elements of Γ are represented on $\lceil \log_2(p+1) \rceil$ bits while $\mathrm{ord}(\Gamma) < p$.
  - The use of *H*(•) is a practical way to remove such a redundancy provided that $\mathrm{ord}(\Gamma) \gg 2^k$.

Subgroup would require to use less bits than the ones we use. So we have redundancy. Hash makes output "more random".

March 25 Diffie-Hellman Key Exchange 48

48