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}^*
 - $-\mid \mathbb{Z}_{11}^* \mid = 10$ whose divisors are 1, 2, 5 (and 10)
 - Subgroup

elements

primitive element

- H_1
- {1}
- α = 1

- H_2
- {1, 10}
- α = 10

- H_5
- {1, 3, 4, 5, 9}
- α = 3, 4, 5, 9

March 25

Diffie-Hellman Key Exchange

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 α = 8 and k = 2, then β = $8^{10/2}$ = 10 mod 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 $|G| = p_1^{e_1} \cdot p_2^{e_2} \cdot ... \cdot p_\ell^{e_\ell}$
 - Run time depends on the size of prime factors
 - The largest prime factor must be in the range 2¹⁶⁰
 - 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, ∀a∈H, a is a generator (Theorem 8.2.4)

March 25

Diffie-Hellman Key Exchange

42

Safe primes vs DLP [→]

- Definition: given a prime $p = 2 \cdot q + 1$, 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 \Rightarrow (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

12

43



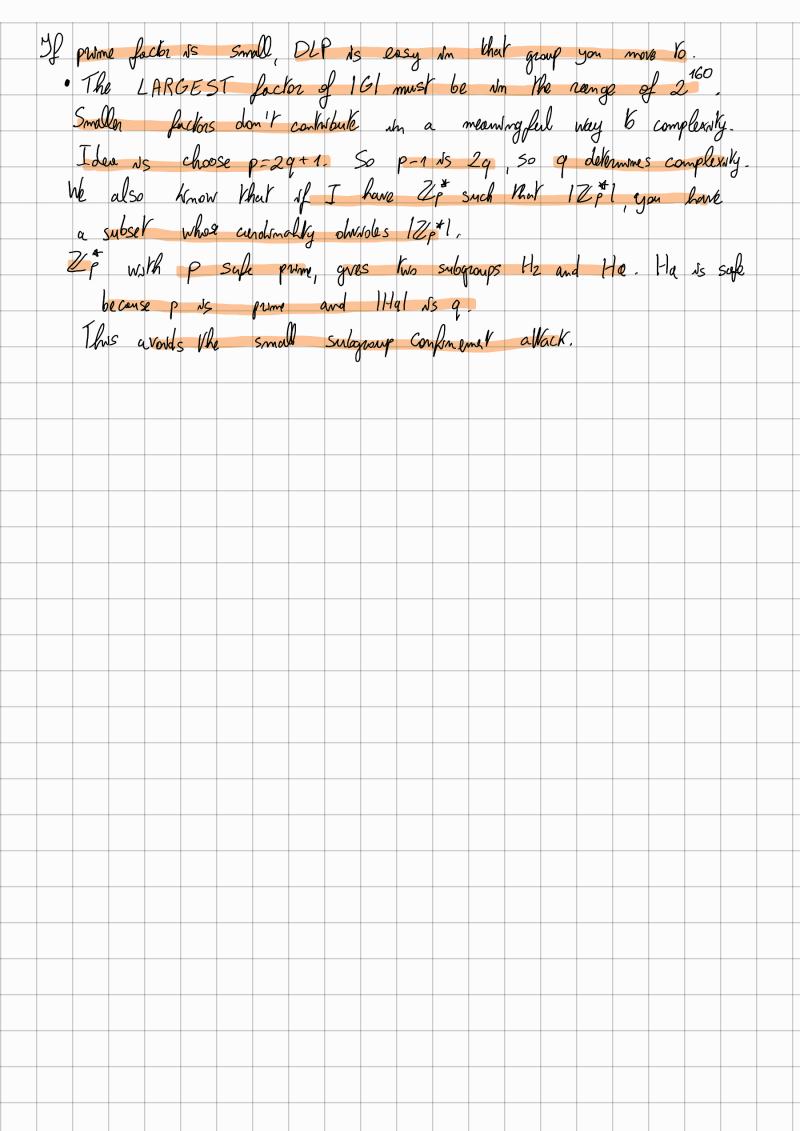
Safe primes vs DLP [■]

- Given \mathbb{Z}_p^* , if p is a safe prime \rightarrow
- $(p-1) = 2 \times q$, with q prime
- Pohling-Hellman decomposes DLP in \mathbb{Z}_p^* into DLP in H_2 and H_q
 - Solving DLP in H₂ 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



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

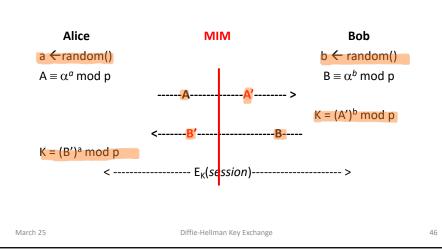
ffie-Hellman Key Exchange

45

45

Small Subgroup Confinement Attack against DHKE

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



· Alice and Bob generale proble key.
· Both compute public key.
· Alice Known K A, but MH modifies at sinte A, same for B in B.

Small Subgroup Confinement Attack against DHKE

- Recall THEOREM 8.2.7
- The attack
 - Consider k that divides $n = |\mathbb{Z}_p^*| = p-1$
 - $-A' \equiv A^{n/k} \equiv (\alpha^a)^{n/k} \equiv (\alpha^{n/k})^a \mod p$
 - $-B' \equiv B^{n/k} \equiv (\alpha^b)^{n/k} \equiv (\alpha^{n/k})^b \mod p$
 - 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 $k \rightarrow$ 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 $H(\bullet)$ 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 $\operatorname{ord}(\Gamma) < p$.
 - − The use of $H(\bullet)$ is a practical way to remove such a redundancy provided that $ord(\Gamma) \gg 2^k$.

"Subgroup Would require to use less buts than the somes we use. So we have redundacy. Itash makes output "more random".

141

iffie-Hellman Key Exchange