

19: DISCRETE LOGARITHM CIPHERS

In this lecture we will look at some ciphers founded on the difficulty of solving the discrete logarithm problem. Throughout, p will be a large prime number and γ will be a primitive root modulo p . So all of the non-zero elements of \mathbb{Z}_p are powers of γ . We will assume that the values of p and γ are published and known to everyone.

19.1 Diffie – Hellman Key Exchange

First we look at how to establish a common secret key so two people can use a symmetric cipher to communicate securely. The method described is the *Diffie – Hellman key exchange*.

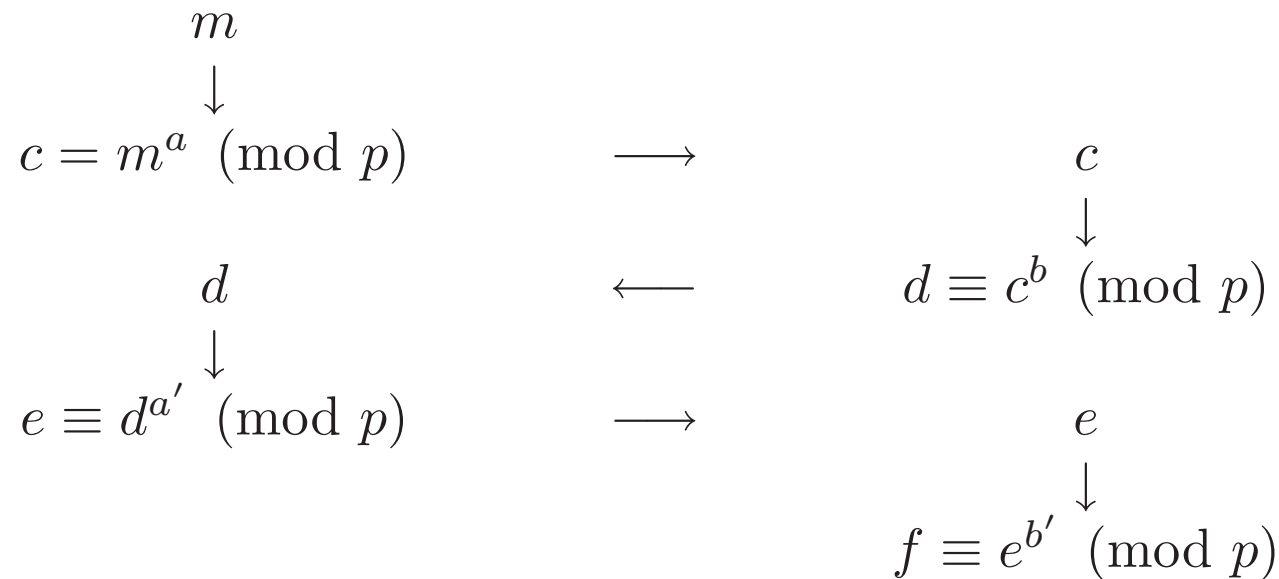
	Alice	Bob
Private	a	b
Public	$A = \gamma^a$	$B = \gamma^b$

$$\text{Key} = A^b \equiv (\gamma^a)^b = (\gamma^b)^a \equiv B^a \pmod{p}.$$

If an enemy can compute discrete logarithms efficiently, then he can find $a = \log_{\gamma} A$ from the published values of p, γ and A . Then he can compute the key as B^a . Diffie and Hellman conjectured but did not prove that finding the value of this key from the published values A and B is equivalent to the discrete logarithm problem.

Shamir showed how we can use this idea to communicate securely without any public keys. Alice and Bob take \mathbb{Z}_p as their alphabet; $m \in \mathbb{Z}_p$.

	Alice		Bob
Private	a		b
Private	a' with $aa' \equiv 1 \pmod{p-1}$		b' with $bb' \equiv 1 \pmod{p-1}$



$e^{b'} \equiv d^{a'b'} \equiv c^{ba'b'} \equiv c^{a'} \equiv m^{aa'} \equiv m \pmod{p}$. So Bob has recovered the plaintext m .

This method has the advantage that no keys have to be published in order for Alice and Bob to communicate. However, it takes three times as long to transmit a message.

19.2 The Elgamal Cipher

Elgamal showed how to adapt the Diffie – Hellman key exchange to give a cipher.

Bob wishes to send encrypted messages to Alice. So Alice chooses a random private key $a \in \mathbb{Z}_{p-1}$; computes $A \equiv \gamma^a \pmod{p}$; and publishes A as her public key. To send a message $m \in \mathbb{Z}_p$, Bob first chooses a random number $b \in \mathbb{Z}_{p-1}$ and sends the pair

$$(c_0, c_1) = (\gamma^b, A^b m) \in \mathbb{Z}_p \times \mathbb{Z}_p .$$

Alice can decipher this by computing $c_1 c_0^{-a} \pmod{p}$. For we have

$$c_1 c_0^{-a} \equiv (\gamma^b)^a \equiv \gamma^{ab} \equiv (\gamma^a)^b \equiv A^b \pmod{p} .$$

So $c_1 c_0^{-a} \equiv m \pmod{p}$.

If an enemy knows one plaintext m and the corresponding ciphertext (c_0, c_1) , then he can find the two public keys $A \equiv \gamma^a \pmod{p}$ and $B \equiv \gamma^b \pmod{p}$ used in the Diffie – Hellman key exchange. Breaking the Elgamal cipher is equivalent to breaking the Diffie – Hellman key exchange. We hope that both are as hard as computing discrete logarithms.