Apply to cryptography

Apply to cryptography

We may use the difficulty of discrete logarithms to encrypt communication.

Question (Public key system, Diffie-Helman key exchange)

Alice wants to encrypt a message so that only Bob can decrypt it, not Eve.

$$\begin{tikzcd} \textit{Alice} \arrow[rr, rightsquigarrow] & {} & \textit{Bob} \\ & \textit{Eve} \arrow[u, dashed, bend right] & \end{tikzcd}$$

Apply to cryptography

1. Alice chooses a large ($\sim 2^{2048}$) prime p such that $\varphi(\varphi(p))$ also has a large prime factor, and finds a primitive root g modulo p. Publishes (p, g), which is the *public key*.

Apply to cryptography

1. Alice chooses a large ($\sim 2^{2048}$) prime p such that $\varphi(\varphi(p))$ also has a large prime factor, and finds a primitive root g modulo p. Publishes (p, g), which is the *public key*.
2. Alice chooses a *private key* a and computes $A := g^a \pmod{p}$. Bob chooses a *private key* b and computes $B := g^b \pmod{p}$.

$$\begin{tikzcd} \text{Alice} \arrow[r, squiggly, bend left, "A"] & \text{Bob} \arrow[l, squiggly, bend left, "B"] \end{tikzcd}$$

Then they exchange A and B (through any channel, probably intercepted by Eve).

3. Alice computes $B^a \pmod{p}$ and Bob computes $A^b \pmod{p}$, both are $\equiv g^{ab} \pmod{p}$. This is their common secret key S.

3. Alice computes $B^a \pmod{p}$ and Bob computes $A^b \pmod{p}$, both are $\equiv g^{ab} \pmod{p}$. This is their common secret key S.
4. Now Alice and Bob can encrypt their communication using the secret key S.

3. Alice computes $B^a \pmod{p}$ and Bob computes $A^b \pmod{p}$, both are $\equiv g^{ab} \pmod{p}$. This is their common secret key S.
4. Now Alice and Bob can encrypt their communication using the secret key S.
5. Eve may know (p, g, A, B). Can Eve find out what S is? This is very hard since finding a (resp. b) from A (resp. B) is difficult.

Some remarks:

- A *Sophie Germain prime* is a prime q such that $p := 2q + 1$ is also a prime. Note that $\varphi(p) = 2q$. Hence, when q is large, p would be a safe prime for the public key system.

Some remarks:

- A *Sophie Germain prime* is a prime q such that $p := 2q + 1$ is also a prime. Note that $\varphi(p) = 2q$. Hence, when q is large, p would be a safe prime for the public key system.
- The primality testing is fast, so generating a public key wouldn't cost too much time.

Some remarks:

- A *Sophie Germain prime* is a prime q such that $p := 2q + 1$ is also a prime. Note that $\varphi(p) = 2q$. Hence, when q is large, p would be a safe prime for the public key system.
- The primality testing is fast, so generating a public key wouldn't cost too much time.
- Alice needs to compute $g^a \pmod{p}$ and $B^a \pmod{p}$, while Bob needs to compute $g^b \pmod{p}$ and $A^b \pmod{p}$. These are modular exponential problems, and we can solve them effectively using binary exponentiation algorithms.

Example 4.8.1

Alice wants to encrypt communication with Bob using Diffie-Helman key exchange. Suppose the public key is $(467, 2)$.

If the private keys of Alice and Bob are $a = 22$ and $b = 33$ respectively. What are A, B and the secret key S?

Apply to cryptography

Public key: $p = 467$, $g = 2$. Private keys: $a = 22$, $b = 33$.

	2	2^2	2^4	2^8	2^{16}	2^{32}	2^{64}	2^{128}	2^{256}
modulo 467	2	4	16	256	156	52	369	264	113

Public key: $p = 467$, $g = 2$. Private keys: $a = 22$, $b = 33$.

	2	2^2	2^4	2^8	2^{16}	2^{32}	2^{64}	2^{128}	2^{256}
modulo 467	2	4	16	256	156	52	369	264	113

1. $A \equiv g^a \pmod{p} \equiv 2^{22} = 2^{2+4+16} \equiv 4 \cdot 16 \cdot 156 \equiv 177 \pmod{467}$,

Public key: $p = 467$, $g = 2$. Private keys: $a = 22$, $b = 33$.

	2	2^2	2^4	2^8	2^{16}	2^{32}	2^{64}	2^{128}	2^{256}
modulo 467	2	4	16	256	156	52	369	264	113

1. $A \equiv g^a \pmod{p} \equiv 2^{22} = 2^{2+4+16} \equiv 4 \cdot 16 \cdot 156 \equiv 177 \pmod{467}$,
2. $B \equiv g^b \pmod{p} \equiv 2^{33} = 2^{1+32} \equiv 2 \cdot 52 \equiv 104 \pmod{467}$,

Public key: $p = 467$, $g = 2$. Private keys: $a = 22$, $b = 33$.

	2	2^2	2^4	2^8	2^{16}	2^{32}	2^{64}	2^{128}	2^{256}
modulo 467	2	4	16	256	156	52	369	264	113

1. $A \equiv g^a \pmod{p} \equiv 2^{22} = 2^{2+4+16} \equiv 4 \cdot 16 \cdot 156 \equiv 177 \pmod{467}$,
2. $B \equiv g^b \pmod{p} \equiv 2^{33} = 2^{1+32} \equiv 2 \cdot 52 \equiv 104 \pmod{467}$,
3. $S \equiv A^b \equiv B^a \equiv g^{ab} \pmod{p}$

   $\equiv 2^{22\cdot 33} \equiv 2^{260} = 2^{4+256} \equiv 16 \cdot 113 \equiv 30 \pmod{467}$.