Ergänzungen 02 zum Skript der Vorlesung

Diskrete Mathematik

Prof. Dr. Wolfgang Konen

RSA für sehr kleine Zahlen (nicht sicher!)

Beispiel: ALICE hat einen sehr kleinen Public Key im Netz stehen: n=1147 und K=k_{pub}=29. Können Sie, wenn Sie wissen, dass ALICE das RSA-Verfahren benutzt, den geheimen Schlüssel S=k_{priv} „erknobeln?

Lösung: Wir wissen, dass n = pq das Produkt zweier Primzahlen p und q sein muss. Mit etwas Probieren finden wir p=31, q=37. Dann ist g=(p-1)(q-1) = 1080. Der geheime Schlüssel S ist das multiplikative Inverse zu K mod 1080. Wir finden dieses S mit dem Algo Euklid:

g	K	floor(n/m)	S	r
1080	29	37	149	-4
29	7	4	-4	1
7	1		1	0

Probe: 149·29+(-4)·1080 = 1. Also ist der geheime Schlüssel **S=149**.

Überlegen Sie sich nun eine geeignete Kodierung, um die Nachricht „CAMPUS“ in Zahlen zu verschlüsseln, chiffrieren Sie dies mit ALICE’s öffentlichem Schlüssel (n,K)=(1147,29) und mit MAPLE. Dechiffrieren Sie das mit dem „erknobelten“ geheimen Schlüssel und mit MAPLE.

Lösung [s. RSA-beispiel.mws]: Wir können mit `> m:=convert("CAMPUS",'bytes');` den Buchstaben die ASCII-Code-Zahlen $m := [67, 65, 77, 80, 85, 83]$ zuweisen. Die Zahlen

müssen wir einzeln[1] an RSA übergeben, da zwei Zahlen hintereinander größer als n=1147 wären. Dann können wir mit

$s_1 = m_1^{29} \bmod n = 25,$

$s_2 = m_2^{29} \bmod n = 548,$ usw.

die geheime Chiffre $sl := [25, 548, 990, 1042, 27, 747]$ ausrechnen und erhalten mit

$d_1 = s_1^{149} \bmod n = 65,$

$d_2 = s_2^{149} \bmod n = 67,$ usw.

die Dechiffrierung, also die Ausgangsnachricht, wieder zurück.

Diffie-Hellman-Protokoll und RSA: Ein wenig zur Historie

Wir hatten in der Vorlesung ja die Frage, wie es sein kann, dass einerseits Diffie und Hellman zu Asymmetric Keys die grundlegende Idee hatten, andererseits nicht mit dem konkreten späteren RSA-Algorithmus aufwarten können. Zur Erklärung bringe ich unten eine Passage, die die Historie ***vor*** der Erfindung von RSA ein wenig beleuchtet. Sie ist eine Zusammenfassung von Texten aus [Singh01]. Da [Singh01] auf Englisch ist, ist diese Zusammenfassung auch auf Englisch …

Key-Distribution Problem: The problem with all traditional cryptography methods is that the key has to be distributed from sender to receiver before safe communication is possible. Since keys should change often, this means considerable amount in personal meetings or courier services → too costly for everyday use. On the other hand, it seems not possible to invent a protocol that overcomes the "catch-22"-situation: Before two people can exchange a secret (an encrypted message) they must already share a secret (the key).

In 1976, the team of Diffie and Hellman came up with a new solution: Hellman invented the first method, how sender and receiver can follow a protocol to establish a secret key over an insecure transmission line. The central feature are one-way functions: such functions are easy to calculate into one direction but very difficult to invert (either because they are non-unique or because there is no "basin of attraction" guiding towards the right solution or both). An example is modular arithmetic: the function $z = z(x) = Y^x \pmod P$ for fixed Y and P is easy to compute, but it is very difficult to find for a given z those values of x which lead to z = z(x).

[1] Wir könnten auch je drei Ziffern an RSA übergeben, das wäre effizienter (nur 4 statt 6 Potenzierungen), aber das macht die Dekodierung etwas aufwändiger. Es wäre aber sicherer, weil keine Bestandteile in der Chiffre auftauchen, die zu einzelnen Buchstaben gehören.

The Hellman protocol works as follows:

ALICE and BOB agree publicly on two numbers Y and P.	
ALICE	BOB
ALICE chooses her secret number A	BOB chooses his secret number B
ALICE computes $a = Y^A \pmod P$	BOB computes $b = Y^B \pmod P$
ALICE transmits a to BOB	BOB transmits b to ALICE
ALICE takes BOB's result and computes $K_A=b^A \pmod P$	BOB takes ALICE's result and computes $K_B=a^B \pmod P$
Miraculously, it turns out that K_A and K_B are the same number, so this number can be used as private key between ALICE and BOB !	

For a third person, EVE, which may hear all transmissions along the line, e.g. who gets all the information Y, P, a, b, it is still extremely difficult (if not impossible) to deduce K_A from this information, provided that the numbers are sufficiently large.

The problem with Hellman's protocol: it requires several messages to be sent back and forth. If ALICE and BOB have a certain time zone difference between them, it may take days until a secret key is established and ALICE finally can send the secret message to BOB.

Public-key cryptography: In 1975, Diffie came up with the idea of asymmetric keying: So long, the key used for encryption was the same as the key used for decryption (symmetric keying). If someone can come up with an asymmetric key, that is an encryption key (public key) different from the decryption key (private key), then ALICE, which want to receive secret messages, can hand out her public key to anybody, and anybody can send her ALICE-encrypted messages. Only ALICE (with her private key) will be able to decrypt these messages.

Mechanical analogy: An open padlock in front of a box can be closed by anybody (encryption, the padlock is ALICE's public key), but it can be opened only by the person who possesses the key (ALICE's private key).

Although Diffie established the main idea of public key cryptography, he was not able to find suitable one-way functions: The public key should establish an one-way function which is not reversible for anybody in the public, but the owner of the public key should have additional information at hand (the accompanying private key) which allows him and only him to reverse the encrypted message.

1977: RSA is invented by Rivest, Shamir and Adleman as the *first public-key method*.

Literatur

- [**Singh01**] Simon Singh: *Geheime Botschaften. Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet*. Dtv, 2001.
  Ein *sagenhaft gutes Buch*!. Absolut spannend wird die Geschichte der Verschlüsselung von der Antike bis heute aufgerollt. Gleichzeitig erfährt man viel über die dahinterstehenden mathematischen Verfahren der Kryptographie und der Codierung, modulare Arithmetik ohne Formeln usw.