Kryptosysteme

Ein Kryptosystem ist ein Tupel $S = (X, K, Y, e, d)$, wobei

Ein Kryptosystem mit Schlüsselverteilung (KSV) ist ein 6-Tupel $V = (X, K, Y, e, d, Pr_K)$, wobei

Kryptosysteme

Dechiffrierbedingung

Kryptosysteme

Surjektivität

Kryptosysteme

Unter einer Chiffre von S versteht man

Kryptosysteme

Ein Kryptosystem heißt possibilistisch sicher, wenn gilt

Kryptosysteme

Sei (S, P_k) ein Kryptosystem mit Schlüsselverteilung. Es heißt informationstheoretisch sicher bezüglich Pr_x, wenn gilt

Definition Verschiebechiffre

Definition Vigenère-Kryptosystem

Block Kryptosystemen

Beschreibe Szenario 2

- $S = (X, K, Y, e, d)$ das zugrundeliegende Kryptosystem ist
- $Pr_K : K \to (0, 1]$ die Schlüsselverteilung
- Für $V = (X, K, Y, e, d, Pr_K)$ schreiben wir auch $S[Pr_K]$
- $Pr_K(k) \in (0, 1]$ also $Pr_K(k) > 0$ für alle $k \in K$
- weiter $Pr_X : X \to [0, 1]$ Klartextverteilung
- $Pr : X \times K \to [0, 1]$ durch $Pr((x, k)) := Pr_X(x) * Pr_K(k)$

- X nicht leere endliche Menge als Klartext
- K nicht leere endliche Menge als Schlüssel
- Y eine Menge als Chiffretexte
- $e : X \times K \to Y$ Verschlüsselungsfunktion
- $d : Y \times K \to X$ Entschlüsselungsfunktion

$\forall y \in Y \exists x \in X, k \in K : y = e(x, k)$

$\forall x \in X \forall k \in K : d(e(x, k), k) = x$

- $\forall y \in Y \forall x \in X \exists k \in K : e(x, k) = y$
- Schlüssel mindestens so lang wie der zu übermittelnde Text
- in jeder Spalte für e kommen alle Chiffretexte vor
- in jeder Zeile für e müssen die Einträge verschieden voneinander sein

die Funktion $e(., k) : X \to Y$, $x \to e(x, k)$ für festes $k \in K$

Eine Verschiebechiffre ist ein Kryptosystem $S = (Z_n, Z_n, Z_n, e, d)$ mit $e(x, k) = (x + k) mod\ n$

- Eintreten von x und y sind unabhängig
- wenn für alle $x \in X, y \in Y$ mit $Pr(y) > 0$ gilt: $Pr(x) = Pr(x|y)$.
- bezüglich jeder beliebigen Klartextverteilung Pr_X informationstheoretisch sicher
- (X, K, Y, e, d) ist possibilistisch sicher und $Pr_K(k) = \frac{1}{|K|}$ für alle $k \in K$
- in jeder Spalte für e alle Chiffretexte vorkommen und die Schlüsselverteilung Pr_K uniform
- für jede Spalte Chiffretextwahrs. separat

Alice möchte Bob mehrere verschiedene Klartexte vorher bekannter und begrenzter Länge übermitteln. Sie verwendet dafür immer denselben Schlüssel. Eva hört die Chiffretexte mit und kann sich sogar einige Klartexte mit dem verwendeten Schlüssel verschlüsseln lassen.

Das Vigenère-Kryptosystem (mit Parametern $(n, S, L) \in \mathbb{N}^3$) ist das Kryptosystem $((\mathbb{Z}_n) \geq L, (\mathbb{Z}_n) \geq S, (\mathbb{Z}_n) \geq L, e, d)$, so dass für alle $s \geq S, l \geq L, x_i, k_j \in \mathbb{Z}_n$ gilt:
$e(x_0...x_{l-1}, k_0...k_{s-1}) = y_0...y_{l-1}$ mit
$y_i = (x_i + k_{i\ mod\ s}) mod\ n$, für alle $0 \geq i < l$.

Block Kryptosysteme

Nenne ein informationstheoretisch sicheres Block-Kryptosystem, das von Eva in Szenarium 2 leicht gebrochen werden kann.

Wann ist ein Kryptosystem possibilistisch sicher bzgl. Szenarium 2

Definition l-Block-Kryptosystem

Ein Substitutions-Permutations-Netzwerk (SPN) ist ein Tupel $N = (m, n, r, s, S, \beta, \kappa)$ wobei

Block Kryptosysteme

In der Vorlesung wurde possibilistische Sicherheit für Szenarium 2 definiert. Nenne ein l-Block-Kryptosystem, das diese Definition erfüllt. Die nötige Schlüsselmenge K hat Größe...

Block Kryptosysteme

Nenne ein Block-Kryptosystem aus der Vorlesung, das gegenwärtig für Szenarium 2 in der Praxis benutzt wird.

Block Kryptosysteme

Beschreibe das Konzept eines l-Unterscheiders

Block Kryptosysteme

Beschreibe das zugehörige Sicherheitsspiel eines l-Unterscheiders

Block Kryptosysteme

Definiere den Vorteil eines l-Unterscheiders.

Ein symmetrisches l-Kryptoschema ist ein Tupel $S = (K, E, D)$, wobei

Ein Kryptosystem $S = (X, K, Y, e, d)$ ist possibilistisch sicher bzgl. Szenarium 2, wenn für jedes $1 \leq r \leq |X|$, jede Folge von paarweise verschiedenen Klartexten $x_1, x_2, ..., x_r \in X$, jeden Schlüssel $k \in K$ und jedes $y \in Y \backslash \{e(x_i, k) | 1 \leq i < r\}$ ein Schlüssel $k' \in K$ existiert mit $e(x_i, k) = e(x_i, k')$ für alle $1 \leq i < r$ und $e(x_r, k') = y$.

Aus Kenntnis von $x \in \{0,1\}^l$ und $y = e(x, k)$ für ein einziges Paar $(x, k) \in X \times K$ kann Eva den Schlüssel $k = x \oplus_l y$ berechnen. Das gilt für das Cäsar-System, das Vigenère-System und das informationstheoretisch sichere **Vernam**-System.

- positive ganzen Zahlen m, n, r und s die Wortanzahl, Wortlängen, Rundenzahl und Schlüssellänge
- $S : \{0,1\}^n \to \{0,1\}^n$ eine bijektive Funktion (S-Box)
- $\beta : \{0, ..., mn-1\} \to \{0, ..., mn-1\}$ selbstinverse Permutation (Bitpermutation)
- $\kappa : \{0,1\}s \times \{0, ..., r\} \to \{0,1\}^{mn}$ Rundenschlüsselfunktion

Sei $l > 0$. Ein l-Block-Kryptosystem ist ein Kryptosystem $S = (\{0,1\}^l, K, \{0,1\}^l, e, d)$ mit $K \subseteq \{0,1\}^s$ für ein $s > 0$.

Triple-DES, AES

Ein Kryptosystem $S = (X, K, Y, e, d)$ ist possibilistisch sicher bzgl. Szenarium 2, wenn für jedes $1 \leq r \leq |X|$, jede Folge von paarweise verschiedenen Klartexten $x_1, x_2, \ldots, x_r \in X$, jeden Schlüssel $k \in K$ und jedes $y \in Y \backslash \{e(x_i, k) | 1 \leq i < r\}$ ein Schlüssel $k' \in K$ existiert mit $e(x_i, k) = e(x_i, k')$ für alle $1 \leq i < r$ und $e(x_r, k') = y$.
Die nötige Schlüsselmenge K hat Größe $\frac{|Y|!}{(|Y|-|X|)!} \geq |X|!$ viele Schlüssel. Mit $X = \{0,1\}^{128}$ gibt es also $\geq 2^{128}!$ viele Schlüssel.

Man entscheidet mit einem Münzwurf, ob Unterscheider U für seine Untersuchungen als $F(.)$ eine zufällige Chiffre $e(., k)$ von Kryptosystem B oder eine zufällige Permutation π von $\{0,1\}^l$ erhalten soll. Dann rechnet U mit F als Orakel und gibt dann seine Meinung ab, ob er sich in der Realwelt oder in der Idealwelt befindet. U „gewinnt", wenn diese Meinung zutrifft.

Ein l-Unterscheider ist ein randomisierter Algorithmus $U(F : \{0,1\}^l \to \{0,1\}^l) : \{0,1\}$, dessen Laufzeit bzw. Ressourcenaufwand durch eine Konstante beschränkt ist. Für ein gegebenes Block-Kryptosystem B ist das gewünschte Verfahren: Programm U sollte 1 liefern, wenn F eine Chiffre $e(., k)$ zu B ist, und 0, wenn $F = \pi$ für eine Permutation $\pi \in P\{0,1\}^l$ ist, die keine B-Chiffre ist.

- $K \subseteq \{0,1\}^s$ endliche Menge (für ein $s \in \mathbb{N}$)
- $E(x : \{0,1\}^{l*}, k : K) : \{0,1\}^{l*}$ randomisierter Algorithmus
- $D(y : \{0,1\}^{l*}, k : K) : \{0,1\}^{l*}$ deterministischer Algorithmus
- Laufzeiten von E und D sind polynomiell beschränkt in der Länge von x bzw. y
- Dechiffrierbedingung: $\forall x \in \{0,1\}^{l*}, k \in K, m \in M_1 \times ... \times M_r$ gilt: $D(E^m(x, k), k) = x$

- der Vorteil von U bzgl. B ist $adv(U, B) := 2(Pr(G_U^B = 1) - \frac{1}{2})$
- Für jeden l-Unterscheider U und jedes l-Block-KS B gilt $-1 \geq adv(U, B) \geq 1$
- Werte $adv(U, B) < 0$ sind uninteressant (Ausgaben können vertauscht werden um positiven Vorteil zu erhalten)

Betriebsarten

Beschreibe die ECB-Betriebsart (Electronic Code Book)

Betriebsarten

Beschreibe die CBC-Betriebsart (Cipher Block Chaining)

Betriebsarten

Beschreibe die R-CBC-Betriebsart (Randomized Cipher Block Chaining)

Betriebsarten

Beschreibe die OFB-Betriebsart (Output FeedBack)

Betriebsarten

Beschreibe die R-CTR-Betriebsart (Randomized CounTeR)

Betriebsarten

Nutze die ECB-Betriebsart. Gebe einen Angreifer an, der die Chiffretexte zweier selbstgewählter Klartexte ohne Kenntnis des Schlüssels unterscheiden kann.

Betriebsarten

Nutze die CBC-Betriebsart. Gebe einen Angreifer an, der die Chiffretexte zweier selbstgewählter Klartexte ohne Kenntnis des Schlüssels unterscheiden kann.

Sei $n, q, t, l \in \mathbb{N}$, A ein l-Angreifer, S ein symmetrisches l-Kryptoschema. Dann heißt $A(n, q, t)$-beschränkt, wenn...

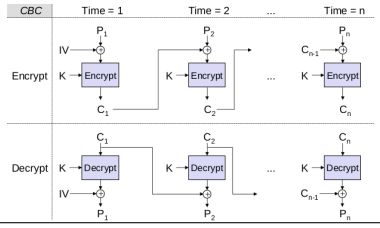
Zahlentheorie

Auf Eingabe $x, y \in \mathbb{N}$ liefert der Euklidische Algorithmus eine ganze Zahlen d mit ...

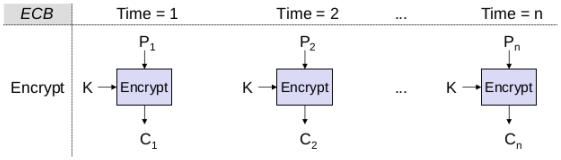
Zahlentheorie

Auf Eingabe $x, y \in \mathbb{N}$ liefert der erweiterte Euklidische Algorithmus (EEA) drei ganze Zahlen d, s, t. Welche Eigenschaften erfüllen diese?

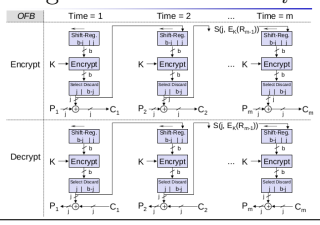
Blöcke in Runden $i = 0, 1, \ldots, m-1$ nacheinander verschlüsselt und das Ergebnis einer Runde wird zur Modifikation des Klartextblocks der nächsten Runde benutzt.



Ein Schlüssel ist ein Schlüssel k von B. Man verschlüsselt einfach die einzelnen Blöcke von x mit B, jedes mal mit demselben Schlüssel k.



Man setzt $k_{-1} = v$, und konstruiert die Rundenschlüssel $k_0, ..., k_{m-1}$ durch iterieren des letzten Rundenschlüssel durch die Verschlüsselungsfunktion von B: $k_i = e_B(k_{i-1}, k)$



Der Initialisierungsvektor $y_{-1} = v \in \{0,1\}^l$ ist nicht mehr Teil des Schlüssels, sondern wird vom Verschlüsselungsalgorithmus einfach zufällig gewählt, und zwar für jeden Klartext immer aufs Neue. Damit der Empfänger entschlüsseln kann, benötigt er v. Daher wird y_{-1} als Zusatzkomponente dem Chiffretext vorangestellt. Damit ist der Chiffretext um einen Block länger als der Klartext, und Eva kennt auch $v = y_{-1}$.

Ein Block $x \in \{0,1\}^l$ wird immer gleich verschlüsselt. Eva kann also ganz leicht nicht-triviale Informationen aus dem Chiffretext erhalten. Zum Beispiel kann sie sofort sehen, ob der Klartext die Form $x = x_1 x_1$, mit $x_1 \in \{0,1\}^l$, hat oder nicht.

Man fasst $\{0,1\}^l$ als äquivalent zur Zahlenmenge $\{0, 1, ..., 2^{l-1}\}$ auf, interpretiert einen l-Bit-String also als Block oder als Zahl, wie es passt. In dieser Menge wählt man eine Zufallszahl r. Man „zählt" von r ausgehend nach oben und berechnet die Rundenschlüssel $k_0, ..., k_{m-1}$ durch Verschlüsseln von $r, r+1, ..., r+m-1$ (modulo 2^l gerechnet) mittelse $B(., k)$. Rundenschlüssel k_i ist also $e_B((r+i) mod\ 2^l, k)$, und Chiffretextblock y_i ist $k_i \oplus_l x_i$.

...die Laufzeit des Experiments G_A^S durch t beschränkt ist, der Algorithmus H (als Orakel) höchstens q mal aufgerufen wird und bei diesen Aufrufen höchstens n Blöcke verwendet werden.

Wird zweimal der Klartext x verschlüsselt, so geschieht dies immer durch denselben Chiffretext $y = E(x, (k, v))$. Dies ist eine Folge der Eigenschaft von CBC, deterministisch zu sein.

1. Für die Ausgabe (d, s, t) gilt $d = ggT(x, y) = s * x + t * y$.
2. Die Anzahl der Schleifendurchläufe ist dieselbe wie beim gewöhnlichen Euklidischen Algorithmus
3. Die Anzahl von Ziffernoperationen ist $O((log\ x)(log\ y))$

$a, b : integer; a \leftarrow |x|; b \leftarrow |y|;$
$while\ b > 0\ repeat$
$\quad (a, b) \leftarrow (b, a\ mod\ b);$
return a

Der Euklidische Algorithmus liefert eine ganze Zahl d, die der größte gemeinsame Teiler von x und y ist.

ZAHLENTHEORIE

Wenn er auf zwei Zahlen mit je n Bits angewendet wird, führt der erweiterte Euklidische Algorithmus $O(\dots)$ Bitoperationen aus.

ZAHLENTHEORIE

Seien a und N teilerfremde natürliche Zahlen. Wie kann man eine ganze Zahl b ermitteln, die die Gleichung $a * b \ mod \ N = 1$ erfüllt?

ZAHLENTHEORIE

Gebe den Algorithmus der Funktion $modexp(x, y, N)$ zur rekursiven Berechnung von $x^y \ mod \ n$ mithilfe der schnellen modularen Exponentiation an.
Dieser Algorithmus führt $O(\dots)$ modulare Multiplikationen aus.

ZAHLENTHEORIE

Vervollständige den Chinesischen Restsatz:
Wenn m und n ... Zahlen sind, dann ist die Abbildung $\Phi : \cdots \to \dots, x \to \dots, \dots$.

ZAHLENTHEORIE

Vervollständige den kleinen Satz von Fermat:
Wenn p ... ist und a in ... liegt, dann gilt: ...

ZAHLENTHEORIE

Vervollständige den Satz von Euler:
Für $m \geq 2$ und x mit ... gilt ....

PRIMZAHLEN

Definiere den Begriff „a ist ein F-Lügner" (für N):
N ist ... und es gilt ....

PRIMZAHLEN

N heißt Carmichael-Zahl, wenn ...

PRIMZAHLEN

Formuliere den Fermat-Test für eine gegebene ungerade Zahl $N \geq 5$:
Wähle... und berechne $c = \dots$. Wenn $c = \dots$ ist, ist die Ausgabe ...., sonst ist sie ....

PRIMZAHLEN

Definiere: $b \in \{1, \dots, N-1\}$ heißt nichttriviale Quadratwurzel der 1 modulo N, wenn...

$(a * b)\ mod\ N = (a\ mod\ N * b\ mod\ N) mod\ N = 1$

$O((log\ x)(log\ y))$

Wenn m und n teilerfremde Zahlen sind, sind die Strukturen $\mathbb{Z}_m \times \mathbb{Z}_n$ und $\mathbb{Z}_{mn}$ isomorph.
Dann ist die Abbildung
$\Phi : \mathbb{Z}_{mn} \ni x \to (x\ mod\ m, x\ mod\ n) \in \mathbb{Z}_m \times \mathbb{Z}_n$
bijektiv. Weiterhin: Wenn $\Phi(x) = (x_1, x_2)$ und $\Phi(y) = (y_1, y_2)$, dann gilt:

- $\Phi(x +_{mn} y) = (x_1 +_m y_1, x_2 +_n y_2)$
- $\Phi(x *_{mn} y) = (x_1 *_m y_1, x_2 *_n y_2)$
- $\Phi(1) = (1, 1)$

function $modexp(x, y, m)$

if $y = 0$ then return 1
if $y = 1$ then return x
$z \leftarrow modexp((x * x) mod\ m, \lfloor y/2 \rfloor, m)$;
if y ist ungerade then $z \leftarrow (z * x) mod\ m$
return z

erfordert $O((log\ m)^2)$ Ziffernoperationen

Für $m \geq 2$ und x mit $ggT(m, x) = 1$ gilt
$x\varphi(m)\ mod\ m = 1$

Wenn p eine Primzahl ist und $a \in \mathbb{Z}_p^*$ liegt, dann gilt $a^{p-1}\ mod\ p = 1$

Eine ungerade zusammengesetzte Zahl N heißt eine Carmichael-Zahl, wenn für alle $a \in \mathbb{Z}_N^*$ die Gleichung $a^{N-1}\ mod\ N = 1$ gilt.

Sei $N \geq 3$ ungerade und zusammengesetzt.
Eine Zahl $a \in \{1, \ldots, N-1\}$ heißt **F-Zeuge** für N, wenn $a^{N-1} mod\ N \neq 1$ gilt.
Eine Zahl $a \in \{1, \ldots, N-1\}$ heißt **F-Lügner** für N, wenn $a^{N-1} mod\ N = 1$ gilt.
Die Menge der F-Lügner nennen wir L_N^F.

Eine Zahl $b \in \{2, \ldots, N-2\}$ mit $b^2\ mod\ N = 1$ heißt eine nicht triviale Quadratwurzel der 1 modulo N.
Bei Primzahlen gibt es solche Zahlen nicht.

Nutze den Fermat-Test, um „Zeugen" dafür anzugeben, dass eine Zahl N zusammengesetzt ist:
Wenn wir eine Zahl a mit $1 \leq a < N$ finden, für die $a^{N-1} mod\ N \neq 1$ gilt, dann ist N definitiv keine Primzahl.
Für eine gegebene ungerade Zahl $N \geq 5$: Wähle $a < 5$ und berechne $c = a^{N-1}\ mod\ N$. Wenn $c \neq 1$ ist, ist die Ausgabe N ist kine Primzahl, sonst ist sie eine Primzahl.

PRIMZAHLEN

Wenn man eine nichttriviale Quadratwurzel b der 1 modulo N gefunden hat, weiß man sicher, dass $N\ldots.$ ist.

PRIMZAHLEN

Definiere den Begriff {qqa ist ein MR-Lügner} (für N): Suche ungerades u und $k \geq 1$ mit $\ldots = \ldots.$ Bilde die Folge $b_0 = \ldots, b_1 = \ldots, \ldots, b_k = \ldots.$ a heißt dann ein MR-Lügner (für N), falls ...

PRIMZAHLEN

Ergänze den Algorithmus von Miller/Rabin (Eingabe $N \geq 5$)

PRIMZAHLEN

Was kann man über das Ein-/Ausgabeverhalten des Miller-Rabin-Algorithmus auf Eingabe $N \geq 5$ (ungerade) sagen? N zusammengesetzt $\Rightarrow \ldots$, N Primzahl $\Rightarrow \ldots$

PRIMZAHLEN

Wie kann man vorgehen, um aus dem Miller-Rabin-Test einen Primzahltest zu erhalten, dessen Fehlerwahrscheinlichkeit höchstens $1/4^l$ beträgt?

PRIMZAHLEN

Formuliere den Primzahlsatz

PRIMZAHLEN

Nach der Ungleichung von Finsler gibt es $\Omega(\ldots)$ Primzahlen im Intervall $[m, 2m)$. Entsprechend muss man für $\mu \in \mathbb{N}$ erwartet nur $O(\ldots)$ Zahlen zufällig aus $[2^{\mu-1}, 2^\mu)$ ziehen, um mindestens eine μ-Bit Primzahl zu erhalten.

PRIMZAHLEN

Zu gegebenem μ soll eine (zufällige) Primzahl im Intervall $[2^{\mu-1}, 2^\mu)$ gefunden werden. Wie geht man vor?

Ein Public-Key-Kryptosystem (X, Y, K, E, D) hat 5 Komponenten

Ein asymmetrisches Kryptoschema ist ein Tupel $S = (X, K, G, E, D)$, wobei

Wir schreiben $N-1 = u * 2^k$, für u ungerade, $k \geq 1$.
Eine Zahl $a, 1 \leq a < N$, heißt ein MR-Lügner für N, wenn $b_0 = 1$ oder in der Folge $b_0, \ldots, b_{k-1}$ zu a kommt $N-1$ vor gilt, $a^u \equiv 1$ oder $a^{u*2^i} \equiv N-1 (mod\ N)$ für ein i mit $0 \leq i < k$

Wenn es eine nichttriviale Quadratwurzel der 1 modulo N gibt, dann ist N zusammengesetzt.

Wenn N zusammengesetzt $\Rightarrow$ gibt es MR-Zeugen.
Wenn N eine Primzahl ist, gibt der MR-Test 0 aus.

suche u ungerade und $k \geq 1$ mit $N-1 = u * 2^k$
wähle zufällig ein a aus $\{1, \ldots, N-1\}$
$b \leftarrow a^u\ mod\ N$
if $b \in \{1, N-1\}$ then return 0
for j from 1 to $k-1$ do
    $b \leftarrow b^2\ mod\ N$
if $b = N-1$ then return 0
if $b = 1$ then return 1
return 1

Primzahlsatz: $lim_{x \to \infty} \frac{\pi(x)}{x \backslash ln\ x} = 1$.
Mit $\pi(x)$ bezeichnen wir die Anzahl der Primzahlen, die nicht größer als x sind.

Tatsächlich ist die Fehlerwahrscheinlichkeit durch $1/4^l$ beschränkt. Dies kann man aber nur durch fortgeschrittene zahlentheoretische Untersuchungen über die erwartete Wahrscheinlichkeit, dass eine zufällige ungerade zusammengesetzte Zahl den l-fach iterierten MiRa-Test übersteht, beweisen.

wiederhole: ... bis Ergebnis ... erscheint. Wie lässt sich die erwartete Anzahl von Bitoperationen für das Finden einer solchen Primzahl abschätzen? $O(\ldots)$.

Ungleichung von Finsler: Für jede ganze Zahl $m \geq 2$ liegen im Intervall $(m, 2m]$ mindestens $m/(3\ ln(2m))$ Primzahlen: $\pi(2m) - \pi(m) \geq \frac{m}{3\ ln(2m)}$.
$\Rightarrow \pi(2m) - \pi(m) = O(m/log\ m)$

- $X, K \supseteq K_{pub} \times K_{priv}$ Mengen,
- $G() : K_{pub} \times K_{priv}$ randomisierter Algorithmus
- $E(x : X, k : K_{pub}) : \{0,1\}^*$ randomisierter Algo.
- $D(y : \{0,1\}^*, k : K_{priv}) : \{0,1\}^*$ determ. Algo.
- Laufzeit ist beschränkt durch eine Konstante,
- die Laufzeiten von E und D sind polynomiell beschränkt
- $\forall x \in X, k \in K_{pub}$ gilt: $D(E^m(x,k), \hat{k}) = x$.

- Klartextmenge X (endlich),
- Chiffretextmenge Y (endlich),
- Schlüsselmenge K, wobei $K \supseteq K_{pub} \times K_{priv}$ für Mengen K_{pub} und K_{priv},
- Verschlüsselungsfunktion $E : X \times K_{pub} \to Y$,
- Entschlüsselungsfunktion $D : Y \times K_{priv} \to X$,
- mit Dechiffrierbedingung: $D(E(x,k), \hat{k}) = x$, für alle $x \in X, (k, \hat{k}) \in K$.

Sei $t \in \mathbb{N}$, A ein Angreifer auf ein asymmetrisches Kryptoschema S. Dann heißt A t-beschränkt, wenn

Sei $\epsilon > 0$. Dann heißt $S(t, \epsilon)$-sicher, wenn

RSA-System

Schlüsselerzeugung: Wähle ... und berechne $N = \ldots$ sowie $\varphi(N) = \ldots$. Der öffentliche Schlüssel von Bob ist (N, e), wobei e die Bedingung ... erfüllt. Der geheime Schlüssel von Bob ist (N, d), mit .... d lässt sich mit folgendem Algorithmus berechnen: ...

RSA-System

Verschlüsseln von $x \in \cdots : y = \ldots$.

RSA-System

Entschlüsseln von $y \in \cdots : z = \ldots$.

RSA-System

Formuliere die zentrale Korrektheitsaussage des RSA-Systems: ...=x, für alle zulässigen Klartextblöcke x.

RSA-System

Beschreibe eine Strategie für RSA-basierte Systeme, mit der verhindert werden kann, dass zwei identische Klartextblöcke bei Verwendung desselben Schlüsselpaars gleich verschlüsselt werden.

Rabin-Kryptosystem

Komponenten des Rabin-Kryptosystems: Zwei große Primzahlen p und q mit .... Der öffentliche Schlüssel ist $N =$..., der private Schlüssel von Bob ist ....

Rabin-Kryptosystem

Verschlüsselung: Alice möchte einen Block $x \in$... an Bob schicken. Sie berechnet $y =$... und sendet y an Bob.

Rabin-Kryptosystem

Entschlüsselung: Wenn Bob das Chiffrat y erhält, berechnet er $z_1, \ldots, z_4$. Wie hängen diese Zahlen mit y zusammen? Mit welchen Formeln berechnet Bob diese vier Zahlen? Was ist der maximale Rechenaufwand? $O(...)$ Bitoperationen.

für jeden t-beschränkten Angreifer A gilt $adv(A, S) \leq \epsilon$.

die Laufzeit des Experiments G_A^S durch t beschränkt ist.

$x \in X = [N] : y = E(x, (N, e)) := x^e \ mod \ N$
(Zu berechnen mit schneller Exponentiation, Rechenzeit $O((log\ N)^3) = O(l^3)$)

Wähe zwei Primzahlen p und q, deren Bitlänge 1/2 der Schlüssellänge ist und das Produkt $N = pq$ sowie $\varphi(N) = (p-1)(q-1)$ berechnet. Es wird eine Zahl $e \in \{3, \ldots, \varphi(N) - 1\}$ mit $ggT(e, \varphi(N)) = 1$ gewählt.

- öffentlicher Schlüssel k ist das Paar (N, e)
- geheimer Schlüssel $\hat{k}$ ist (N, d) mit multiplikativ Inversen $d < \varphi(N) modulo\ \varphi(N)$ von e
- es gilt $ed\ mod\ \varphi(N) = 1$
- Berechnungsaufwand $O((log\ N)^4) = O(l^4)$

Korrektheit/Dechiffrierbedingung von RSA: Wenn $ed\ mod\ \varphi(N) = 1$ gilt, dann haben wir $x^{ed}\ mod\ N = x$, für alle $x \in [N]$.

$y \in Y : z = D(y, (N, d)) := y^d \ mod \ N$
(Zu berechnen mit schneller Exponentiation, Rechenzeit $O((log\ N)^3) = O(l^3)$)

Wähle zwei verschiedene zufällige große Primzahlen p und q mit $p \equiv q \equiv 3(mod\ 4)$, also Primzahlen, die um 1 kleiner als ein Vielfaches von 4 sind. Berechne $N = pq$. Der öffentliche Schlüssel ist $k = N$; der geheime Schlüssel ist $\hat{k} = (p, q)$.

Es ist Empfohlen, beim Arbeiten mit RSA den Klartext x durch das Anhängen eines nicht ganz kurzen Zufallsstrings zu randomisieren. Wenn dieser angehängte Zufallsstring die gleiche Länge wie x hat, ist der Chiffretext genauso lang wie bei ElGamal.

Quadratwurzeln b berechnen mit $b^2 mod\ N = y$. Faktoren p und q bekannt. Berechne Quadratwurzeln $r := y^{(p+1)/4} mod\ p$ und $s := y^{(q+1)/4} mod\ q$. Mit der konstruktiven Variante des chinesischen Restsatzes:

- $z_1 \equiv r(mod\ p)$ und $z_1 \equiv s(mod\ q)$
- $z_2 \equiv r(mod\ p)$ und $z_2 \equiv q - s(mod\ q)$
- $z_3 \equiv p - r(mod\ p)$ und $z_3 \equiv s(mod\ q)$
- $z_4 \equiv p - r(mod\ p)$ und $z_4 \equiv q - s(mod\ q)$

insgesamt Zeit $O((log\ N)^3)$

Verschlüsselung eines Blocks, der eine Zahl $x < N$ ist:
$y := x^2 \ mod \ N$
benötigt nur Zeit $O((log\ N)^2)$

RABIN-KRYPTOSYSTEM

Formuliere die zentrale Sicherheitsaussage des Rabin-Kryptosystems: ...

ELGAMAL-KRYPTOSYSTEM

Definiere die Exponentiation mit Basis g und den Logarithmus zur Basis g jeweils mit Definitions- und Wertebereich.

ELGAMAL-KRYPTOSYSTEM

Um die Schlüssel festzulegen, wählt Bob zufällig eine geheime Zahl $b \in \ldots$. Der öffentliche Schlüssel ist ... mit $B = \ldots$

ELGAMAL-KRYPTOSYSTEM

Verschlüsselung von Klartextblock $x \in \ldots$ mit öffentlichem Schlüssel: ...

ELGAMAL-KRYPTOSYSTEM

Entschlüsselung von Chiffretext $\ldots \in \ldots$ mithilfe von b :$\ldots$

ELGAMAL-KRYPTOSYSTEM

Gebe das Diffie-Hellman-Problem an Zu Input ..., ... finde ....

ELGAMAL-KRYPTOSYSTEM

Zur Sicherheit des ElGamal-Kryptosystems lässt sich feststellen: Eve kann alle bzgl. G und g verschlüsselten Nachrichten effizient entschlüsseln genau dann wenn ...

ELGAMAL-KRYPTOSYSTEM

Wieso verwendet man in der Praxis lieber Systeme, die auf elliptischen Kurven basieren, als solche, die auf diskreten Logarithmen beruhen?

Sei $p > 3$ eine Primzahl, seien $A, B \in \mathbb{Z}_p$ mit .... Die elliptische Kurve $E_{A,B}$ besteht aus der Menge aller Lösungen ... der Gleichung ... sowie einem zusätzlichen Punkt ... (genannt „der unendliche Punkt").

Definition Hasse-Schranke

Gegeben sei eine zyklische Gruppe $(G, \circ, e)$ der Ordnung (Kardinalität) N mit erzeugendem Element g. $exp_g: \ldots \to \ldots, \ldots \to \ldots log_g: \ldots \to \ldots, \ldots \to \ldots$ Für die Berechnung der Exponentiation werden $O(\ldots)$ Gruppenoperationen benötigt.

Welche der oberen Möglichkeiten die richtige (ausgewählte) ist, hängt vom Zufall ab, der die Auswahl von x steuert. Jede der 4 Quadratwurzeln von y hat dieselbe Wahrscheinlichkeit $1/4$, als x gewählt worden zu sein.
Eva muss also nur $ggT(x - z, N)$ berechnen! Damit gelingt es ihr mit Wahrscheinlichkeit $1/2$, die Faktoren von N zu ermitteln. Durch l-fache Wiederholung desselben Experiments lässt sich die Erfolgswahrscheinlichkeit auf $1 - \frac{1}{2^l}$ erhöhen.

Wir nehmen an, dass die Menge der möglichen Botschaften (Binärstrings) eine Teilmenge von G ist.
Um eine Botschaft $x \in G$ zu verschlüsseln, wählt Alice eine Zufallszahl a aus $\{2, \ldots, |G| - 2\}$ und berechnet $A = g^a$
Weiter berechnet sie $y := B^a \circ x$
Der Chiffretext ist (A, y)

Es wird eine zyklische Gruppe $(G, \circ, e)$ mit einem erzeugenden Element g benötigt, sowie $N = |G|$, so dass das zugehörige DH-Problem schwer zu lösen ist.
Ein Element b wird zufällig aus $\{2, \ldots, |G| - 2\}$ gewählt, und es wird mittels schneller Exponentiation $B = g^b$ berechnet.
Der öffentliche Schlüssel ist $k_{pub} = (G, g, B)$,
der geheime Schlüssel ist b bzw. $k_{priv} = (G, g, b)$

Die Idee ist, dass $k = g^{ab}$ ist, wobei nur Alice a kennt und nur Bob b. Über den öffentlichen Kanal laufen die Gruppenelemente g^a und g^b. Eva hat also das Problem, aus g^a und g^b den Wert g^{ab} zu berechnen.
Zu Input $k = g^{ab}$, wobei nur Alice a kennt und nur Bob b kennt, finde g^a und g^b.

Bob kennt die Gruppe G und g, sowie A und y (von Alice) sowie seinen geheimen Schlüssel b. Er berechnet $A^b = (g^a)^b = k$. Dann berechnet er das Gruppenelement $z = k^{-1} \circ y$, mit Hilfe der effizienten Invertierung und Gruppenoperation in G.

- kleinere Schlüsselmenge bei deutlich höherer Komplexität
- nur durch Brute Force und Ausprobieren möglich zu knacken
- geringer Aufwand bei hoher Sicherheit

Eva kann effizient entschlüsseln, also aus B, A und y die Nachricht x berechnen, die zum Chiffretext (A, y) geführt hat wenn Sie das DH-Problem für G lösen kann

Sei E elliptische Kurve über $\mathbb{Z}_p$. Dann gilt $p + 1 - 2\sqrt{p} \leq |E| \leq p + 1 + 2\sqrt{p}$.

Sei $p > 3$ eine Primzahl, seien $A, B \in \mathbb{Z}_p$ mit $4A^3 + 27B^3 \neq 0$. Die elliptische Kurve $E_{A,B}$ besteht aus der Menge aller Lösungen $(x, y) \in \mathbb{Z}_p^2$ der Gleichung $y^2 = x^3 + Ax + B$ sowie einem zusätzlichen Punkt O (genannt „der unendliche Punkt").