

Introduction to Public Key Cryptography

→ Symmetric Cryptography revisited. → Most symmetric algorithms like AES and 3DES are fast, secure & used, but there are some issues.



1. Key Distribution Problem: Key must be established between Alice & Bob under secure channel which may not be possible.
2. Number of Keys: Due to large number of keys → grows in number of n users → $\frac{n(n-1)}{2}$ keys where every user shares $(n-1)$ keys securely.
3. No Protection Against Cheating by Alice or Bob.

not of concern

→ Symmetric: Same secret key used for encrypt & decrypt + encrypt & decrypt f^{-1} very similar

→ Principles of Asymmetric Cryptography - Encryption & Key Transfer: Not necessary that key possessed by person encrypting message is secret.



In practice: Symmetric keys must be shorter than asymmetric keys & need to be padded to some length as input for asymmetric keys.

Consider combination of secret key for symmetric encryption along asymmetric encryption as a joint gain.

Do not expect msg as input → Key Encapsulation Mechanism

generate random values for symmetric secret key on their own and fed into asymmetric encryption F .

Bob runs decapsulator to decrypt and change key.

Public Keys → Long Keys → Block Computation

→ Asymmetric schemes built using One-way F: F is easy to compute on every input but hard to reverse any output of random input.

→ Def: of One-way F: F is One-way if:

$$y = f(x) \text{ is computationally feasible}$$

$$x = f^{-1}(y) \text{ is infeasible}$$

Ex: RSA based Integer Factorization, Discrete Logarithm Problem.

→ Hybrid Protocols must be used to ensure Best of Both Worlds

→ Public Key Algorithm Families:

Algorithm Family	Cryptosystems	Security Level (bits)
Integer Factorization	RSA, Rabin, DSA, ElGamal	(80) 128 bits
Discrete logarithm	DH, DSA, ElGamal	(1024) 3072 bits
Elliptic Curve	ECDH, ECDSA	(160) 1024 bits
Symmetric-key	AES	(80) 128 bits
		(112) 192 bits
		(256) 256 bits

Each can be used for key establishment, non-repudiation & decryption.

→ Main Security Mechanisms of Public-Key Algorithms:

1. Key Establishment: Protocols of establishing secret keys over insecure channels.

2. Non-repudiation: Providing non-repudiation realized by Digital Signature Algorithms (DSA).

3. Integrity: DSA also ensures integrity.

4. Identification: Identify entities using challenge-and-response protocols + signatures.

5. Encryption

→ All 3 families based on number theoretic F's → Very long operational keys → Highly secure (Security level of n bits → Best attack requires 2^n steps)

Essential Number Theory:

gcd of $r_0, r_1 \in \mathbb{Z}^+$ $\text{gcd}(r_0, r_1)$ is the largest $a \in \mathbb{Z}^+$ at. $a|r_0$ and $a|r_1$.

→ For large numbers, Euclid's Algorithm used: if r_0 & r_1 have common divisor g , any linear combination of r_0 and r_1 is divisible by g → $\text{gcd}(r_0, r_1) = \text{gcd}(r_0 - r_1, r_1) = g$ for $r_0 > r_1$.

Say $\text{gcd}(r_0, r_1) = g$. Since $g|r_0$ and $g|r_1$, $r_0 = g \cdot x$ and $r_1 = g \cdot y$ where $x > y$ and $x > y$ are coprime numbers.

→ If we continue this process, $\text{gcd}(r_0, r_1) = \text{gcd}(r_0 - r_1, r_1) = \text{gcd}(r_0 - 2r_1, r_1) = \dots$

$$= \text{gcd}(r_0 - Mr_1, r_1) \text{ where } Mr_1 > 0$$

$$\begin{aligned} &\downarrow \\ &\text{To choose Max } m: \quad \text{gcd}(r_0, r_1) = \text{gcd}(r_0 - Mr_1, r_1) \\ &\quad = \text{gcd}(r_0, r_0 \text{ mod } r_1) \quad r_0 \text{ mod } r_1 < r_1 \\ &\quad \text{we swap} \end{aligned}$$

Reduce Problem of Finding gcd of 2 numbers → Find gcd of 2 smaller numbers

gcd(r_0, r_1) = ... = gcd($r_0, 0$) = r_0

→ Extension of Euclid's: complete modular inverses used in PKE

→ EEA computes $\text{gcd}(r_0, r_1) = s \cdot r_0 + t \cdot r_1$ for $s, t \in \mathbb{Z}$

Diophantine Equation

→ Derivation of Recursive Formulae for s_i & t_i :

$$r_{i-2} = [s_{i-2}]r_0 + [t_{i-2}]r_1 = q_{i-1}r_{i-1} + r_i \Rightarrow r_i = r_{i-2} - q_{i-1}r_{i-1}$$

$$r_{i-1} = [s_{i-1}]r_0 + [t_{i-1}]r_1$$

$$\begin{aligned} &\dots \\ &s_i = s_{i-2} - q_{i-1}s_{i-1} \\ &t_i = t_{i-2} - q_{i-1}t_{i-1} \end{aligned}$$

$$\begin{aligned} &\text{Starting Values: } s_0 = t_1 = 1 \\ &s_1 = r_0 = 0 \\ &t_0 = r_1 = 1 \\ &\text{Valid for: } b_i = t_{i-2} - q_{i-1}t_{i-1} \\ &i = 2, 3, \dots \end{aligned}$$

→ Show how EEA can be used to compute multiplicative inverses in $\mathbb{F}(2^n)$

→ Inputs of EEA are in $P(x)$ and irreducible $P(x)$

EEA computes polynomials $s(x)$ and $t(x)$ alongside $\text{gcd}(P(x), A(x)) = 1$

$$\begin{aligned} &P(x) \text{ is irreducible} \Rightarrow \text{gcd} = 1 \\ &S(x)P(x) + t(x)A(x) = \text{gcd}(P(x), A(x)) = 1 \end{aligned}$$

$$\begin{aligned} &S(x)0 + t(x)A(x) \equiv 1 \pmod{P(x)} \\ &t(x) \equiv A^{-1}(x) \pmod{P(x)} \end{aligned}$$

Extended Euclidean Algorithm (EEA)
Input: positive integers r_0 and r_1 such that $r_0 > r_1$
Output: $\text{gcd}(r_0, r_1)$, as well as s and t such that $\text{gcd}(r_0, r_1) = s \cdot r_0 + t \cdot r_1$

Initialization:
 $i = 1$
 $r_0 = r_0$
 $r_1 = r_1$
 $s_0 = 1$
 $t_0 = 0$
 $s_1 = 0$
 $t_1 = 1$

Algorithm:
1.0 DO
1.1 $i = i + 1$
1.2 $r_i = r_{i-2} \text{ mod } r_{i-1}$
1.3 $s_i = s_{i-2} - q_{i-1}s_{i-1}$
1.4 $t_i = t_{i-2} - q_{i-1}t_{i-1}$
1.5 $q_{i-1} = r_{i-2} - q_{i-1}r_{i-1}$
1.6 WHILE $r_i \neq 0$
2. RETURN $\text{gcd}(r_0, r_1) = r_{i-1}$
2.1 $s = s_{i-1}$
2.2 $t = t_{i-1}$

Implementation:
1.0 $i = 1$
1.1 $r_0 = r_0$
1.2 $r_1 = r_1$
1.3 $s_0 = 1$
1.4 $t_0 = 0$
1.5 $q_0 = r_0 \text{ div } r_1$
1.6 $r_2 = r_0 - q_0 \cdot r_1$
1.7 $s_1 = s_0 - q_0 \cdot s_1$
1.8 $t_1 = t_0 - q_0 \cdot t_1$
1.9 $q_1 = r_1 \text{ div } r_2$
1.10 $r_3 = r_1 - q_1 \cdot r_2$
1.11 $s_2 = s_1 - q_1 \cdot s_2$
1.12 $t_2 = t_1 - q_1 \cdot t_2$
1.13 $q_2 = r_2 \text{ div } r_3$
1.14 $r_4 = r_2 - q_2 \cdot r_3$
1.15 $s_3 = s_2 - q_2 \cdot s_3$
1.16 $t_3 = t_2 - q_2 \cdot t_3$
1.17 $q_3 = r_3 \text{ div } r_4$
1.18 $r_5 = r_3 - q_3 \cdot r_4$
1.19 $s_4 = s_3 - q_3 \cdot s_4$
1.20 $t_4 = t_3 - q_3 \cdot t_4$
1.21 $q_4 = r_4 \text{ div } r_5$
1.22 $r_6 = r_4 - q_4 \cdot r_5$
1.23 $s_5 = s_4 - q_4 \cdot s_5$
1.24 $t_5 = t_4 - q_4 \cdot t_5$
1.25 $q_5 = r_5 \text{ div } r_6$
1.26 $r_7 = r_5 - q_5 \cdot r_6$
1.27 $s_6 = s_5 - q_5 \cdot s_6$
1.28 $t_6 = t_5 - q_5 \cdot t_6$
1.29 $q_6 = r_6 \text{ div } r_7$
1.30 $r_8 = r_6 - q_6 \cdot r_7$
1.31 $s_7 = s_6 - q_6 \cdot s_7$
1.32 $t_7 = t_6 - q_6 \cdot t_7$
1.33 $q_7 = r_7 \text{ div } r_8$
1.34 $r_9 = r_7 - q_7 \cdot r_8$
1.35 $s_8 = s_7 - q_7 \cdot s_8$
1.36 $t_8 = t_7 - q_7 \cdot t_8$
1.37 $q_8 = r_8 \text{ div } r_9$
1.38 $r_{10} = r_8 - q_8 \cdot r_9$
1.39 $s_9 = s_8 - q_8 \cdot s_9$
1.40 $t_9 = t_8 - q_8 \cdot t_9$
1.41 $q_9 = r_9 \text{ div } r_{10}$
1.42 $r_{11} = r_9 - q_9 \cdot r_{10}$
1.43 $s_{10} = s_9 - q_9 \cdot s_{10}$
1.44 $t_{10} = t_9 - q_9 \cdot t_{10}$
1.45 $q_{10} = r_{10} \text{ div } r_{11}$
1.46 $r_{12} = r_{10} - q_{10} \cdot r_{11}$
1.47 $s_{11} = s_{10} - q_{10} \cdot s_{11}$
1.48 $t_{11} = t_{10} - q_{10} \cdot t_{11}$
1.49 $q_{11} = r_{11} \text{ div } r_{12}$
1.50 $r_{13} = r_{11} - q_{11} \cdot r_{12}$
1.51 $s_{12} = s_{11} - q_{11} \cdot s_{12}$
1.52 $t_{12} = t_{11} - q_{11} \cdot t_{12}$
1.53 $q_{12} = r_{12} \text{ div } r_{13}$
1.54 $r_{14} = r_{12} - q_{12} \cdot r_{13}$
1.55 $s_{13} = s_{12} - q_{12} \cdot s_{13}$
1.56 $t_{13} = t_{12} - q_{12} \cdot t_{13}$
1.57 $q_{13} = r_{13} \text{ div } r_{14}$
1.58 $r_{15} = r_{13} - q_{13} \cdot r_{14}$
1.59 $s_{14} = s_{13} - q_{13} \cdot s_{14}$
1.60 $t_{14} = t_{13} - q_{13} \cdot t_{14}$
1.61 $q_{14} = r_{14} \text{ div } r_{15}$
1.62 $r_{16} = r_{14} - q_{14} \cdot r_{15}$
1.63 $s_{15} = s_{14} - q_{14} \cdot s_{15}$
1.64 $t_{15} = t_{14} - q_{14} \cdot t_{15}$
1.65 $q_{15} = r_{15} \text{ div } r_{16}$
1.66 $r_{17} = r_{15} - q_{15} \cdot r_{16}$
1.67 $s_{16} = s_{15} - q_{15} \cdot s_{16}$
1.68 $t_{16} = t_{15} - q_{15} \cdot t_{16}$
1.69 $q_{16} = r_{16} \text{ div } r_{17}$
1.70 $r_{18} = r_{16} - q_{16} \cdot r_{17}$
1.71 $s_{17} = s_{16} - q_{16} \cdot s_{17}$
1.72 $t_{17} = t_{16} - q_{16} \cdot t_{17}$
1.73 $q_{17} = r_{17} \text{ div } r_{18}$
1.74 $r_{19} = r_{17} - q_{17} \cdot r_{18}$
1.75 $s_{18} = s_{17} - q_{17} \cdot s_{18}$
1.76 $t_{18} = t_{17} - q_{17} \cdot t_{18}$
1.77 $q_{18} = r_{18} \text{ div } r_{19}$
1.78 $r_{20} = r_{18} - q_{18} \cdot r_{19}$
1.79 $s_{19} = s_{18} - q_{18} \cdot s_{19}$
1.80 $t_{19} = t_{18} - q_{18} \cdot t_{19}$
1.81 $q_{19} = r_{19} \text{ div } r_{20}$
1.82 $r_{21} = r_{19} - q_{19} \cdot r_{20}$
1.83 $s_{20} = s_{19} - q_{19} \cdot s_{20}$
1.84 $t_{20} = t_{19} - q_{19} \cdot t_{20}$
1.85 $q_{20} = r_{20} \text{ div } r_{21}$
1.86 $r_{22} = r_{20} - q_{20} \cdot r_{21}$
1.87 $s_{21} = s_{20} - q_{20} \cdot s_{21}$
1.88 $t_{21} = t_{20} - q_{20} \cdot t_{21}$
1.89 $q_{21} = r_{21} \text{ div } r_{22}$
1.90 $r_{23} = r_{21} - q_{21} \cdot r_{22}$
1.91 $s_{22} = s_{21} - q_{21} \cdot s_{22}$
1.92 $t_{22} = t_{21} - q_{21} \cdot t_{22}$
1.93 $q_{22} = r_{22} \text{ div } r_{23}$
1.94 $r_{24} = r_{22} - q_{22} \cdot r_{23}$
1.95 $s_{23} = s_{22} - q_{22} \cdot s_{23}$
1.96 $t_{23} = t_{22} - q_{22} \cdot t_{23}$
1.97 $q_{23} = r_{23} \text{ div } r_{24}$
1.98 $r_{25} = r_{23} - q_{23} \cdot r_{24}$
1.99 $s_{24} = s_{23} - q_{23} \cdot s_{24}$
2.00 $t_{24} = t_{23} - q_{23} \cdot t_{24}$
2.01 $q_{24} = r_{24} \text{ div } r_{25}$
2.02 $r_{26} = r_{24} - q_{24} \cdot r_{25}$
2.03 $s_{25} = s_{24} - q_{24} \cdot s_{25}$
2.04 $t_{25} = t_{24} - q_{24} \cdot t_{25}$
2.05 $q_{25} = r_{25} \text{ div } r_{26}$
2.06 $r_{27} = r_{25} - q_{25} \cdot r_{26}$
2.07 $s_{26} = s_{25} - q_{25} \cdot s_{26}$
2.08 $t_{26} = t_{25} - q_{25} \cdot t_{26}$
2.09 $q_{26} = r_{26} \text{ div } r_{27}$
2.10 $r_{28} = r_{26} - q_{26} \cdot r_{27}$
2.11 $s_{27} = s_{26} - q_{26} \cdot s_{27}$
2.12 $t_{27} = t_{26} - q_{26} \cdot t_{27}$
2.13 $q_{27} = r_{27} \text{ div } r_{28}$
2.14 $r_{29} = r_{27} - q_{27} \cdot r_{28}$
2.15 $s_{28} = s_{27} - q_{27} \cdot s_{28}$
2.16 $t_{28} = t_{27} - q_{27} \cdot t_{28}$
2.17 $q_{28} = r_{28} \text{ div } r_{29}$
2.18 $r_{30} = r_{28} - q_{28} \cdot r_{29}$
2.19 $s_{29} = s_{28} - q_{28} \cdot s_{29}$
2.20 $t_{29} = t_{28} - q_{28} \cdot t_{29}$
2.21 $q_{29} = r_{29} \text{ div } r_{30}$
2.22 $r_{31} = r_{29} - q_{29} \cdot r_{30}$
2.23 $s_{30} = s_{29} - q_{29} \cdot s_{30}$
2.24 $t_{30} = t_{29} - q_{29} \cdot t_{30}$
2.25 $q_{30} = r_{30} \text{ div } r_{31}$
2.26 $r_{32} = r_{30} - q_{30} \cdot r_{31}$
2.27 $s_{31} = s_{30} - q_{30} \cdot s_{31}$
2.28 $t_{31} = t_{30} - q_{30} \cdot t_{31}$
2.29 $q_{31} = r_{31} \text{ div } r_{32}$
2.30 $r_{33} = r_{31} - q_{31} \cdot r_{32}$
2.31 $s_{32} = s_{31} - q_{31} \cdot s_{32}$
2.32 $t_{32} = t_{31} - q_{31} \cdot t_{32}$
2.33 $q_{32} = r_{32} \text{ div } r_{33}$
2.34 $r_{34} = r_{32} - q_{32} \cdot r_{33}$
2.35 $s_{33} = s_{32} - q_{32} \cdot s_{33}$
2.36 $t_{33} = t_{32} - q_{32} \cdot t_{33}$
2.37 $q_{33} = r_{33} \text{ div } r_{34}$
2.38 $r_{35} = r_{33} - q_{33} \cdot r_{34}$
2.39 $s_{34} = s_{33} - q_{33} \cdot s_{34}$
2.40 $t_{34} = t_{33} - q_{33} \cdot t_{34}$
2.41 $q_{34} = r_{34} \text{ div } r_{35}$
2.42 $r_{36} = r_{34} - q_{34} \cdot r_{35}$
2.43 $s_{35} = s_{34} - q_{34} \cdot s_{35}$
2.44 $t_{35} = t_{34} - q_{34} \cdot t_{35}$
2.45 $q_{35} = r_{35} \text{ div } r_{36}$
2.46 $r_{37} = r_{35} - q_{35} \cdot r_{36}$
2.47 $s_{36} = s_{35} - q_{35} \cdot s_{36}$
2.48 $t_{36} = t_{35} - q_{35} \cdot t_{36}$
2.49 $q_{36} = r_{36} \text{ div } r_{37}$
2.50 $r_{38} = r_{36} - q_{36} \cdot r_{37}$
2.51 $s_{37} = s_{36} - q_{36} \cdot s_{37}$
2.52 $t_{37} = t_{36} - q_{36} \cdot t_{37}$
2.53 $q_{37} = r_{37} \text{ div } r_{38}$
2.54 $r_{39} = r_{37} - q_{37} \cdot r_{38}$
2.55 $s_{38} = s_{37} - q_{37} \cdot s_{38}$
2.56 $t_{38} = t_{37} - q_{37} \cdot t_{38}$
2.57 $q_{38} = r_{38} \text{ div } r_{39}$
2.58 $r_{40} = r_{38} - q_{38} \cdot r_{39}$
2.59 $s_{39} = s_{38} - q_{38} \cdot s_{39}$
2.60 $t_{39} = t_{38} - q_{38} \cdot t_{39}$
2.61 $q_{39} = r_{39} \text{ div } r_{40}$
2.62 $r_{41} = r_{39} - q_{39} \cdot r_{40}$
2.63 $s_{40} = s_{39} - q_{39} \cdot s_{40}$
2.64 $t_{40} = t_{39} - q_{39} \cdot t_{40}$
2.65 $q_{40} = r_{40} \text{ div } r_{41}$
2.66 $r_{42} = r_{39} - q_{40} \cdot r_{41}$
2.67 $s_{41} = s_{40} - q_{40} \cdot s_{41}$
2.68 $t_{41} = t_{40} - q_{40} \cdot t_{41}$
2.69 $q_{41} = r_{41} \text{ div } r_{42}$
2.70 $r_{43} = r_{40} - q_{41} \cdot r_{42}$
2.71 $s_{42} = s_{41} - q_{41} \cdot s_{42}$
2.72 $t_{42} = t_{41} - q_{41} \cdot t_{42}$
2.73 $q_{42} = r_{42} \text{ div } r_{43}$
2.74 $r_{44} = r_{41} - q_{42} \cdot r_{43}$
2.75 $s_{43} = s_{42} - q_{42} \cdot s_{43}$
2.76 $t_{43} = t_{42} - q_{42} \cdot t_{43}$
2.77 $q_{43} = r_{43} \text{ div } r_{44}$
2.78 $r_{45} = r_{42} - q_{43} \cdot r_{44}$
2.79 $s_{44} = s_{43} - q_{43} \cdot s_{44}$
2.80 $t_{44} = t_{43} - q_{43} \cdot t_{44}$
2.81 $q_{44} = r_{44} \text{ div } r_{45}$
2.82 $r_{46} = r_{43} - q_{44} \cdot r_{45}$
2.83 $s_{45} = s_{44} - q_{44} \cdot s_{45}$
2.84 $t_{45} = t_{44} - q_{44} \cdot t_{45}$
2.85 $q_{45} = r_{45} \text{ div } r_{46}$
2.86 $r_{47} = r_{44} - q_{45} \cdot r_{46}$
2.87 $s_{46} = s_{45} - q_{45} \cdot s_{46}$
2.88 $t_{46} = t_{45} - q_{45} \cdot t_{46}$
2.89 $q_{46} = r_{46} \text{ div } r_{47}$
2.90 $r_{48} = r_{45} - q_{46} \cdot r_{47}$
2.91 $s_{47} = s_{46} - q_{46} \cdot s_{47}$
2.92 $t_{47} = t_{46} - q_{46} \cdot t_{47}$
2.93 $q_{47} = r_{47} \text{ div } r_{48}$
2.94 $r_{49} = r_{46} - q_{47} \cdot r_{48}$
2.95 $s_{48} = s_{47} - q_{47} \cdot s_{48}$
2.96 $t_{48} = t_{47} - q_{47} \cdot t_{48}$
2.97 $q_{48} = r_{48} \text{ div } r_{49}$
2.98 $r_{50} = r_{47} - q_{48} \cdot r_{49}$
2.99 $s_{49} = s_{48} - q_{48} \cdot s_{49}$
3.00 $t_{49} = t_{48} - q_{48} \cdot t_{49}$
3.01 $q_{49} = r_{49} \text{ div } r_{50}$
3.02 $r_{51} = r_{48} - q_{49} \cdot r_{50}$
3.03 $s_{50} = s_{49} - q_{49} \cdot s_{50}$
3.04 $t_{50} = t_{49} - q_{49} \cdot t_{50}$
3.05 $q_{50} = r_{50} \text{ div } r_{51}$
3.06 $r_{52} = r_{49} - q_{50} \cdot r_{51}$
3.07 $s_{51} = s_{50} - q_{50} \cdot s_{51}$
3.08 $t_{51} = t_{50} - q_{50} \cdot t_{51}$
3.09 $q_{51} = r_{51} \text{ div } r_{52}$
3.10 $r_{53} = r_{50} - q_{51} \cdot r_{52}$
3.11 $s_{52} = s_{51} - q_{51} \cdot s_{52}$
3.12 $t_{52} = t_{51} - q_{51} \cdot t_{52}$
3.13 $q_{52} = r_{52} \text{ div } r_{53}$
3.14 $r_{54} = r_{51} - q_{52} \cdot r_{53}$
3.15 $s_{53} = s_{52} - q_{52} \cdot s_{53}$
3.16 $t_{53} = t_{52} - q_{52} \cdot t_{53}$
3.17 $q_{53} = r_{53} \text{ div } r_{54}$
3.18 $r_{55} = r_{52} - q_{53} \cdot r_{54}$
3.19 $s_{54} = s_{53} - q_{53} \cdot s_{54}$
3.20 $t_{54} = t_{53} - q_{53} \cdot t_{54}$
3.21 $q_{54} = r_{54} \text{ div } r_{55}$
3.22 $r_{56} = r_{53} - q_{54} \cdot r_{55}$
3.23 $s_{55} = s_{54} - q_{54} \cdot s_{55}$
3.24 $t_{55} = t_{54} - q_{54} \cdot t_{55}$
3.25 $q_{55} = r_{55} \text{ div } r_{56}$
3.26 $r_{57} = r_{54} - q_{55} \cdot r_{56}$
3.27 $s_{56} = s_{55} - q_{55} \cdot s_{56}$
3.28 $t_{56} = t_{55} - q_{55} \cdot t_{56}$
3.29 $q_{56} = r_{56} \text{ div } r_{57}$
3.30 $r_{58} = r_{55} - q_{56} \cdot r_{57}$
3.31 $s_{57} = s_{56} - q_{56} \cdot s_{57}$
3.32 $t_{57} = t_{56} - q_{56} \cdot t_{57}$
3.33 $q_{57} = r_{57} \text{ div } r_{58}$
3.34 $r_{59} = r_{56} - q_{57} \cdot r_{58}$
3.35 $s_{58} = s_{57} - q_{57} \cdot s_{58}$
3.36 $t_{58} = t_{57} - q_{57} \cdot t_{58}$
3.37 $q_{58} = r_{58} \text{ div } r_{59}$
3.38 $r_{60} = r_{57} - q_{58} \cdot r_{59}$
3.39 $s_{59} = s_{58} - q_{58} \cdot s_{59}$
3.40 $t_{59} = t_{58} - q_{58} \cdot t_{59}$
3.41 $q_{59} = r_{59} \text{ div } r_{60}$
3.42 $r_{61} = r_{58} - q_{59} \cdot r_{60}$
3.43 $s_{60} = s_{59} - q_{5$